

Tätigkeitsbericht 2021 des Datenschutzbeauftragten des Landessportverbandes für das Saarland e.V. (LSVS)

Inhaltsverzeichnis

| | |
|--|---|
| 1. Management Summary..... | 2 |
| 2. Situation des Datenschutzes beim LSVS..... | 3 |
| 3. Aufgaben des Datenschutzes..... | 3 |
| 3.1 Übersicht der Aufgabengebiete..... | 3 |
| 3.2 Beratung und Stellungnahmen..... | 4 |
| 3.3 Betroffenenrechte..... | 4 |
| 3.4 Verarbeitungstätigkeiten und Risikofolgenabschätzung..... | 4 |
| 3.5 Auftragsverarbeitung..... | 4 |
| 3.6 Änderungen in der Gesetzgebung mit Datenschutzrelevanz..... | 5 |
| 3.6.1 Infektionsschutzgesetz (IfSG)..... | 5 |
| 3.6.2 Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG)..... | 5 |
| 3.6.3 Angemessenheitsbeschluss UK..... | 5 |
| 3.7 Einsatz von US-Anbietern..... | 5 |
| 3.7.1 Google Fonts..... | 5 |
| 3.7.2 Facebook und instagram..... | 6 |
| 3.7.3 MS 365 Datenschutzrechtliche Probleme:..... | 6 |
| 3.8 Mitarbeiterschulungen..... | 6 |
| 3.9 Durchführung von Prüfungen..... | 7 |
| 3.10 Datenschutzverletzungen..... | 8 |
| 4. Kommunikation mit der Landesbeauftragten für den Datenschutz..... | 8 |
| 5. Zusammenfassung..... | 8 |

Abkürzungsverzeichnis:

| | |
|-----|--|
| AVV | Auftragsverarbeitungs-Vertrag |
| DSB | Datenschutzbeauftragter |
| DSK | Datenschutzkoordinator |
| TOM | Technische und organisatorischen Maßnahmen |
| pbD | Personenbezogene Daten |
| VVT | Verzeichnis von Verarbeitungstätigkeiten |

1. Management Summary

Mit diesem Tätigkeitsbericht erhält der Vorstand des Landessportverbandes für das Saarland e.V. (LSVS) einen Nachweis zur Einhaltung der DS-GVO und weiteren Datenschutzvorschriften.

Mit der EU-Datenschutz-Grundverordnung (DS-GVO) wird das Datenschutzrecht europaweit einheitlich geregelt. Die Verordnung ist am 25.05.2016 in Kraft getreten und gilt gem. Art. 99 Abs. 2 DS-GVO ab dem 25.05.2018 unmittelbar in allen EU Mitgliedstaaten. Entsprechend verpflichtet die DS-GVO den LSVS und seine Auftragsverarbeiter zur Gewährleistung des grundrechtlichen Schutzes der Rechte der Betroffenen sowie gegen unbefugte Zugriffe durch Dritte die dafür angemessenen technischen und organisatorischen Maßnahmen (bspw. in Art. 32, 28 Abs. 3 lit. d DS-GVO) auszuwählen und im Rahmen der Technikgestaltung und datenschutzfreundlicher Voreinstellungen gem. Art. 25 DS-GVO einzusetzen und regelmäßig zu überprüfen (Art. 32 Abs. 1 lit. d). Vereine und Verbände sind für die Einhaltung der Grundsätze der Verarbeitung nach Art. 5 Abs. 1, 24 DS-GVO verantwortlich und müssen dessen Einhaltung gemäß Art. 5 Abs. 2 DS-GVO nachweisen.

Herausforderungen für den Datenschutz beim LSVS: 2021 kam es beim LSVS zu einer größeren Umstrukturierung. 2 Vorstände nahmen ihre Arbeit auf und als Kontrollgremium wurde ein Aufsichtsrat eingerichtet. Nach Anpassung dieser organisatorischen Änderungen in der Datenschutzdokumentation wurde das VVT einer Inventur unterzogen.

In einer „Leitlinie Datenschutz“ wurden durch den Vorstand die für den Datenschutz relevanten Rollen und Funktionen der Mitarbeitenden festgeschrieben. Neu geschaffen wurde die Stelle eines Datenschutzkoordinators zur operativen Umsetzung der DS-GVO.

IT-seitig wurde für den DSB ein VPN Zugang und für die Datenschutzorganisation (DSB + DSK) ein eigenes Laufwerk eingerichtet, damit künftig auf einer einheitlichen Datenbasis gearbeitet werden kann. Im Dokumentenmanagement wurde die Hinterlegung der AV-Verträge initiiert, so dass AV-Verträge künftig zentral vorgehalten werden können.

Gesetzesänderungen im Jahr 2021:

- Das **Infektionsschutzgesetz (IfSG)** trat am 01.01.2021 in Kraft. Wesentlich für Unternehmen ist deren Verpflichtung, Gesundheitsdaten der Mitarbeiter zu erfassen und temporär zu speichern und daraus ggf. resultierende Maßnahmen zu ergreifen. Mehr dazu in Kapitel 3.6.1.
- Das **Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG)** trat am 01.12.2021 in Kraft. Dieses Gesetz wurde notwendig zur Anpassung der Datenschutzbestimmungen des Telekommunikationsgesetzes (TKG) und des Telemediengesetzes (TMG) an die DS-GVO. TKG und TMG enthalten fortan keine Datenschutzbestimmungen. Beachten Sie bitte die sich daraus ergebenden Maßnahmen in 3.6.2.

Angemessenheitsbeschluss UK: Die EU-Kommission hat am 28. Juni 2021 einen Angemessenheitsbeschluss gem. Art. 45 DS-GVO für das Vereinigte Königreich UK erlassen, wodurch UK als sicheres Drittland anerkannt wird. Somit können personenbezogene Daten auch nach dem Brexit ungehindert von der EU ins Vereinigte Königreich transferiert werden.

Angaben zu internen Anfragen: Anfragen von Mitarbeitern zu Datenschutzthemen gab es zu den Themen:

- Prüfung DS-GVO Konformität: Luca-App, Social Media Kanäle, MS teams
- Gestaltung von Einwilligungs- und Verschwiegenheitserklärungen
- Datenschutzkonforme Weiterleitung pbD an die GEMA
- Fragen zum Datenschutz im Zusammenhang mit der Neugestaltung der Webseite des LSVS

Angaben zu externen Anfragen: Betroffenenanfragen gab es im Berichtszeitraum keine. Ebenso gab es keine Anfragen oder Prüfungen durch die saarländischen Datenschutzaufsichtsbehörde.

Datenschutzverletzungen 2021: Keine

Bericht zu Schulungsmaßnahmen: 2021 wurde eine Datenschutzbildung für die Personalabteilung durchgeführt. Zum Ende des Jahres wurde ein Schulungsplan abgestimmt, so dass im ersten Quartal 2022 allen Mitarbeitenden ein Angebot einer Datenschutzbildung unterbreitet werden kann.

2. Situation des Datenschutzes beim LSVS

Die Einhaltung und Umsetzung der DS-GVO wird fortlaufend sichergestellt. Die vorhandene Dokumentation besteht aus:

- einem Verzeichnis von Verarbeitungstätigkeiten (VVT),
- einem Verzeichnis von Verarbeitungstätigkeiten Auftragsverarbeiter (VVT-AV),
- Dokumentation der techn. und organisatorischen Maßnahmen (TOM),
- Datenschutzerklärung auf der Webseite,
- Verträge zur Auftragsverarbeitung mit Kunden und Dienstleistern,
- Mustertexte für: Einwilligung, Information bei Datenerhebung, Verpflichtung auf Vertraulichkeit.

3. Aufgaben des Datenschutzes

3.1 Übersicht der Aufgabengebiete

Kernaufgabe des Datenschutzes ist es, darauf hinzuwirken, die datenschutzrechtlichen Anforderungen im allgemeinen Geschäftsbetrieb, im Geschäftsverkehr mit Kunden, in Projekten und in den IT-Systemen durch alle Geschäftsbereiche im Unternehmen und gegenüber den Mitarbeitenden zu beachten und einzuhalten. Wesentliche Aspekte der Aufgabenerfüllung des DSB erstrecken sich daher auf die Projektberatung, die Durchführung von datenschutzrechtlichen Kontrollhandlungen, Datenschutzaudits, die Beantwortung von Anfragen, die Erstellung datenschutzrechtlicher Einschätzungen sowie die Durchführung von Schulungsmaßnahmen.

3.2 Beratung und Stellungnahmen

Die Mitarbeiter wurden schriftlich über aktuelle Entwicklungen im Datenschutz informiert. Themen- und Beratungsschwerpunkte waren:

- Informationspflichten bei der Datenerhebung,
- Einwilligungen der Eltern Minderjähriger,
- DS-GVO konforme Nutzung von Social Media Kanälen,
- Datenschutzhinweise in Projekten und bei Veranstaltungen,
- Verpflichtungserklärung zur Vertraulichkeit.

Schulungsmaßnahmen: 2021 wurde eine Datenschutzbildung für die Personalabteilung durchgeführt. Zum Ende des Jahres wurde ein Schulungsplan abgestimmt, so dass im ersten Quartal 2022 allen Mitarbeitenden ein Angebot einer Datenschutzbildung unterbreitet werden kann.

3.3 Betroffenenrechte

Auskunfts- und Löschersuchen gab es keine.

3.4 Verarbeitungstätigkeiten und Risikofolgenabschätzung

Eine Inventur des VVT wurde durchgeführt. Eine Inventur muss im Rahmen des Datenschutzmanagements regelmäßig erfolgen. Eine zusätzliche Notwendigkeit ergab sich aus der Umstrukturierung des LSVS im Jahre 2021.

Vorgehensweise der VVT-Inventur: Die Geschäftsbereichsleiter erhielten einen Auszug aus dem VVT mit den ihrem Geschäftsbereich zugeordneten Verarbeitungstätigkeiten zur Prüfung und Überarbeitung. Damit wurde erreicht, dass Verarbeitungstätigkeiten nach der Umstrukturierung dem richtigen Geschäftsbereich zugeordnet werden. Da bis Jahresende nicht alle Rückmeldungen aus den Fachbereichen vorlagen, musste die Inventur auf Q1/2022 ausgeweitet werden.

3.5 Auftragsverarbeitung

Einen Auftragsverarbeitungs-Vertrag (AV-Vertrag) muss nach DS-GVO jedes Unternehmen abschließen, das personenbezogene Daten im Auftrag – also von einem Dienstleister - verarbeiten lässt.

Für den LSVS ist das gleich in zweierlei Hinsicht wichtig. Erstens zur Unterstützung interner Prozesse (z.B. IT-Support) und zweitens in seiner Rolle als Auftragsverarbeiter seiner Mitgliedsverbände.

Art, Umfang und Anzahl aktiver Auftragsverarbeitung sind dem "Verzeichnis von Verarbeitungstätigkeiten Auftragsverarbeiter" (VVT-AV) zu entnehmen. Berichtswerte Ereignisse mit Auftragsverarbeitern gab es keine.

3.6 Änderungen in der Gesetzgebung mit Datenschutzrelevanz

3.6.1 Infektionsschutzgesetz (IfSG)

Das **Infektionsschutzgesetz (IfSG)** trat am 01.01.2021 in Kraft. Wesentlich für Unternehmen ist deren Verpflichtung, Gesundheitsdaten der Mitarbeiter zu erfassen und temporär zu speichern und daraus ggf. resultierende Maßnahmen zu ergreifen.

Erwähnenswert ist insbes. die zum 24.11.2021 in Kraft getretene Verarbeitung des „G-Status“ im Beschäftigtenverhältnis. § 28b IfSG enthält nunmehr eine bundesweite gesetzliche Grundlage für eine 3G-Zugangsregelung am Arbeitsplatz sowie eine ausdrückliche Verarbeitungsbe fugnis durch den Arbeitgeber. Die Regelungen des § 28b Abs. 1 IfSG gelten zunächst bis Ablauf des 19.03.2022.

In diesem Zusammenhang wurde für die Mitarbeiter eine Datenschutzrechtliche Information bei der Datenerhebung formuliert. Die Verarbeitung wurde ins VVT aufgenommen.

3.6.2 Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG)

Am 01.12.2021 ist das neue TTDSG in Kraft getreten. Im TTDSG werden die Datenschutzregelungen des TKG und des TMG zusammengeführt. Zwei Regelungen haben praktische Relevanz:

- § 3 TTDSG löst § 88 TKG ab. Hier geht es um den Schutz des Fernmeldegeheimnisses, weshalb Einwilligungen angepaßt werden müssen.
- § 25 TTDSG löst die Regelung des § 15 Abs. 3 TMG ab. Jetzt steht ausdrücklich im Gesetz (was ohnehin schon gemacht wurde), dass Betreiber von Webseiten eine ausdrückliche Einwilligung zum Setzen von nicht notwendigen Cookies einholen müssen.
 - Notwendige Cookies: Z.B.
 - Keine vorausgewählte Kästchen
 - Informationspflichten: Lebensdauer der Cookies; Art, Zweck und Einsatzweise; Hinweis auf Zugriff Dritter (Dienstleister, der die Cookies verarbeitet); Hinweis Widerrufsmöglichkeit; Möglichkeit der Änderung der Einstellungen; Hinweis Datenschutzerklärung.
 - Nicht notwendige Cookies (aktive Einwilligung erforderlich): Z.B. Einordnung von Nutzerprofilen für optimierte Werbeanzeigen, Messung der conversion rate.

3.6.3 Angemessenheitsbeschluss UK

Die EU-Kommission hat am 28. Juni 2021 einen Angemessenheitsbeschluss gem. Art. 45 DSGVO für das Vereinigte Königreich UK erlassen, wodurch UK als sicheres Drittland anerkannt wird. Somit können pbD auch nach dem Brexit ungehindert von der EU ins Vereinigte Königreich transferiert werden.

3.7 Einsatz von US-Anbietern

3.7.1 Google Fonts

Aufgrund eines aktuellen Urteils des [LG München](#) sollten Sie prüfen, ob Webauftritte Schriften (z.B. Google Fonts) lokal einbinden oder extern nachladen. Sofern letzteres der Fall sein soll-

te, müsste diese schnellstmöglich abgestellt werden und durch lokales Einbinden ersetzt werden.

3.7.2 Facebook und Instagram

Facebook und Instagram sind beide keine eigenständigen Unternehmen mehr, sondern Marken der neuen Dachorganisation Meta Platforms Ireland Limited. Die Datenschutzerklärung auf der Webseite musste entsprechend angepasst werden (Meta Platforms Ireland Limited, 4 Grand Canal Square, Grand Canal Harbour, Dublin 2).

3.7.3 MS 365 Datenschutzrechtliche Probleme:

- Eine Mehrheit von Aufsichtsbehörden sieht datenschutzrechtliche Probleme in der Nutzung von MS 365:
 - Microsoft hat seinen Sitz in den USA (EuGH Urteil zu Schrems II).
 - Microsoft verarbeitet Daten zu eigenen Zwecken. Ein Vertrag zur gemeinsamen Verantwortlichkeit wäre erforderlich. Einen solchen Vertrag gibt es allerdings nicht.
 - Microsoft leitet manche Daten an Drittanbieter ohne Unterauftragsverhältnis weiter.
 - Microsoft verarbeitet Telemetriedaten ohne erkennbare Rechtsgrundlage.
 - Datenverarbeitungen sind für Mitarbeiter intransparent.
 - Microsoft bietet Möglichkeiten der Leistungs- und Verhaltenskontrolle von Mitarbeitern
- Maßnahmen zur Reduzierung des Sanktionsrisikos:
 - Speicherung von Online Service Terms (OST) und Data Processing Addendum (DPA) in der Datenschutzerklärung,
 - Berechtigungskonzept,
 - Konzept zur Aufbewahrung, Löschung, Archivierung und Backup,
 - Risikobewertung (Schwellwertanalyse); ggf. Nachweis, dass keine Alternative verfügbar ist,
 - Betriebsvereinbarung zu MS 365.

Fazit: Eine zu 100% datenschutzkonforme Nutzung ist immer noch nicht möglich.

3.8 Mitarbeiterschulungen

Aufgabe des Datenschutzbeauftragten ist die Sensibilisierung der Mitarbeiter im Umgang mit personenbezogenen Daten. Häufig sind sie auch hinsichtlich Spam-Mails und der Nachrichtenlage zur Cyberkriminalität etc. verunsichert.

Eine Präsenzschulung erfolgte mit der Personalabteilung. Zum Ende des Jahres wurde mit den Führungskräften ein Schulungsplan abgestimmt, so dass im ersten Quartal 2022 allen Mitarbeitenden ein Angebot einer Datenschutzeschulung angeboten werden kann.

3.9 Durchführung von Prüfungen

Im Berichtszeitraum stand die Weiterführung des Verarbeitungsverzeichnisses und die Kontrolle der AV-Verträge im Vordergrund. Schwerpunkte der Prüfungen und Kontrollen im Berichtszeitraum waren:

- Überprüfung, ob die datenschutzrechtlichen Vorschriften eingehalten werden, z.B. ob Daten rechtmäßig gespeichert und verarbeitet werden, oder ob die Wahrung der Rechte der Betroffenen sichergestellt werden kann (u.a. Auskunfts-, Berichtigungs-, Sperrungs- und Löschungsrecht);
- Prüfung, ob die technischen und organisatorischen Maßnahmen - hierbei insbesondere die IT-Sicherheitsmaßnahmen - zur Wahrung des Datenschutzes umgesetzt und befolgt werden, u.a.:
 - Risikoorientierte Benutzer- und Berechtigungsverwaltung;
 - Einhaltung der Funktionstrennung;
 - Einhaltung des Vier-Augen-Prinzips;
 - Vornahme von Protokollierungen;
 - Überwachung der ordnungsgemäßen Einführung und Anwendung der IT-Programme, von der Kontrolle eines korrekten Vorgehens bei der Programmauswahl und -erstellung, Installation eines Verfahrens über die Datenspeicherung, -verarbeitung und -weitergabe bis zum Ergebnis der Datenverarbeitung und der Löschung der Daten.
- Mitwirkung bei der datenschutzrechtlichen Gestaltung von AV-Verträgen mit Auftragnehmern sowie die Kontrolle der Einhaltung der technischen und organisatorischen Maßnahmen beim LSVS.
- Die Fachbereiche wurden unterwiesen, Risikobewertungen sachgerecht durchzuführen. Durch die Bearbeitung der techn. und organ. Maßnahmen wurde folgendes erreicht:
 - Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte (Zugangskontrolle),
 - Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern (Datenträgerkontrolle),
 - Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten (Speicherkontrolle),
 - Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte (Benutzerkontrolle),
 - Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben (Zugriffskontrolle),
 - Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (Übertragungskontrolle),

- Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind (Eingabekontrolle),
- Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und die Integrität der Daten geschützt werden (Transportkontrolle),
- Gewährleistung, dass eingesetzte Systeme im Störfall wiederhergestellt werden können (Wiederherstellbarkeit),
- Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit),
- Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität),
- Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
- Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
- Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können (Trennbarkeit).

Im Ergebnis der Prüfungen wurden keine Verstöße gegen datenschutzrechtliche Vorgaben festgestellt. Insbesondere kann die Einhaltung der vorgegeben technischen und organisatorischen Maßnahmen bestätigt werden.

3.10 Datenschutzverletzungen

Datenpannen / Schutzverletzungen wurden im Berichtseitraum nicht gemeldet.

4. Kommunikation mit der Landesbeauftragten für den Datenschutz

Anfragen der Landesbeauftragten für Datenschutz gab es im Berichtszeitraum keine. Auch seitens des LSVS gab es keine Anfragen an die Aufsichtsbehörde.

5. Zusammenfassung

Datenschutzmanagement/Datenschutzorganisation: Regeln und Anweisungen zum Umgang mit personenbezogenen Daten (pbD) wurden eingeführt. Verantwortlichkeiten und Zuständigkeiten sind festgelegt. Die Datenschutz-Dokumentation ist vollständig und aktuell.

Sicherheit der Verarbeitung: Technische und organisatorische Maßnahmen zur Sicherheit pbD sind eingeführt und dokumentiert. Die Sicherheit der Daten ist gewährleistet.

Aufbewahrung und Löschung von Daten: Die Aufbewahrungsfristen und somit die Löschvorgaben für pbD wurden bei der Entstehung von (Geschäfts)-Prozessen ausführlich berücksichtig-

sichtigt. Durch technische und organisatorische Maßnahmen ist sichergestellt, dass pbD nur so lange gespeichert werden, wie diese erforderlich sind.

Kundeneinwilligungen: Erforderliche Einwilligungen bei der Verarbeitung von Kundendaten werden berücksichtigt. Entsprechende Formulare stehen dem Vertrieb und Service zur Verfügung.

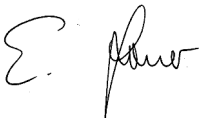
Rechte der betroffenen Person: Die Informationspflichten gegenüber Betroffenen (i.d.R. Kunden und Beschäftigte) werden erfüllt. Entsprechende Informationsblätter wurden erstellt. Die gesetzlich vorgeschriebenen Informationen haben die Kunden erhalten. Prozesse zur Wahrung der Rechte der Betroffenen (Auskunft, Widerruf, Datenschutz-Verletzung etc.) wurden eingeführt.

Auftragsverarbeiter: Relevante Auftragsverarbeiter (Dienstleister) sind sorgfältig ausgewählt. Datenschutzrechtliche Verträge wurden abgeschlossen.

Datenschutz-Folgenabschätzung: Eine Datenschutz-Folgenabschätzung mußte nicht durchgeführt werden. Risikobewertungen bei der Verarbeitung pbD wurden durchgeführt und dokumentiert. Mit Ausnahme des US-Datentransfers besteht kein hohes Risiko für Betroffene bei der Verarbeitung von pbD.

Fazit: Die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz pbD sind beim LSVS erfüllt. Die DS-GVO wurde vollständig umgesetzt und deren Umsetzung wird fortlaufend sichergestellt.

Nalbach, 25.03.2022



Elmar Lauer
Datenschutzbeauftragter

Lauer Datenschutz
Fußbachstraße 25
66809 Nalbach

<https://www.lauer-datenschutz.de>

