

Landeswohlfahrtsverband Hessen

Leitlinie zur Datenschutzorganisation beim Landeswohlfahrtsverband Hessen (Datenschutzleitlinie)

(Stand: 23.06.2021)

Inhaltsverzeichnis

Vorwort.....	4
1. Grundsätze.....	4
2. Verantwortlichkeiten	5
2.1 Behördenleitung	5
2.2 Beschäftigte	5
3. Die/Der behördliche Datenschutzbeauftragte	5
3.1 Grundsatz.....	5
3.2 Aufgaben.....	6
4. Datenschutzkoordinatorinnen und -koordinatoren	6
5. Datenschutzkontrolle	6
6. Verpflichtung/Schulung der Beschäftigten	7
7. Grundsätze für die Verarbeitung personenbezogener Daten	7
7.1 Rechtmäßigkeit der Verarbeitung	7
7.1.1 Datenverarbeitung aufgrund rechtlicher Verpflichtung.....	7
7.1.2 Einwilligung in die Datenverarbeitung	7
7.1.3 Datenverarbeitung für eine vertragliche Beziehung.....	7
7.1.4 Datenverarbeitung für die Zwecke des Beschäftigungsverhältnisses	8
7.1.5 Verarbeitung besonders schutzwürdiger Daten.....	8
7.1.6 Datenverarbeitung aufgrund von Kollektivvereinbarungen	8
7.1.7 Datenverarbeitung aufgrund berechtigten Interesses	8
7.1.8 Automatisierte Einzelentscheidungen	9
7.2 Zweckbindung	9
7.3 Betroffenenrechte.....	9
7.3.1 Recht auf Auskunft.....	9
7.3.2 Recht auf Berichtigung.....	9
7.3.3 Recht auf Löschung	9
7.3.4 Recht auf Einschränkung der Verarbeitung.....	9
7.3.5 Recht auf Widerspruch.....	10
7.3.6 Recht auf Datenübertragbarkeit	10
7.4 Datenvermeidung und Datensparsamkeit.....	10
7.5 Aufbewahrungsfristen und Löschung.....	10
7.6 Sachliche Richtigkeit und Datenaktualität	10
7.7 Vertraulichkeit.....	10

Leitlinie zur Datenschutzorganisation beim Landeswohlfahrtsverband Hessen

7.8 Datensicherheit	11
7.9 Rechenschafts- und Dokumentationspflichten	11
7.9.1 Verzeichnis der Verarbeitungstätigkeiten und Datenschutzfolgenabschätzung	12
7.9.2 Dokumentation der technischen und organisatorischen Maßnahmen	12
7.9.3 Dokumentation von Anfragen und Anträgen zur Wahrung der Betroffenenrechte	12
7.9.4 Datenschutzerklärung	12
8. Erhebung/Verarbeitung von personenbezogenen Daten	12
9. Datenhaltung/-löschung.....	13
10. Übermittlung personenbezogener Daten	13
11. Verarbeitung von personenbezogenen Daten im Auftragsverhältnis.....	14
12. Datenschutzverstöße.....	14
13. Beschaffung von Hard- und Software	14
14. Telekommunikation und Internet.....	15
15. Inkrafttreten	15

Vorwort

Datenschutz und Datensicherheit besitzen seit jeher einen hohen Stellenwert beim Landeswohlfahrtsverband Hessen (im Folgenden LWV Hessen genannt).

Dazu zählen - als Grundsätze unserer Aufgabenwahrnehmung - die Einhaltung der einschlägigen Datenschutzvorschriften durch unsere Beschäftigten (im Sinne des § 23 Abs. 8 HDSIG), der verantwortungsvolle Umgang mit den in unserem Hause verarbeiteten sensiblen personenbezogenen Daten, ein hohes Maß an technischer Sicherheit und die Wahrung der Rechte von Betroffenen.

Diejenigen, die uns ihre Daten anvertrauen, müssen jederzeit sicher sein können, dass wir diese Daten stets mit großer Achtsamkeit, Sorgfalt und streng nach den geltenden Gesetzen und Vorschriften verarbeiten.

Diese Leitlinie soll helfen, die Bedeutung des Datenschutzes beim LWV Hessen und die damit verbundenen Prozesse transparent darzustellen.

In diesem Sinne regelt diese Leitlinie die datenschutzkonforme Verarbeitung personenbezogener Daten und die beim LWV Hessen bestehenden Verantwortlichkeiten und Abläufe, wobei alle Beschäftigten uneingeschränkt zur Einhaltung dieser Leitlinie verpflichtet sind.

1. Grundsätze

Der LWV Hessen verpflichtet sich im Rahmen seiner gesellschaftlichen und sozialen Verantwortung zur Einhaltung der einschlägigen Datenschutzgesetze und -vorschriften.

Diese Datenschutzleitlinie gilt für den gesamten LWV Hessen, bestehend aus der Hauptverwaltung Kassel, den Regionalverwaltungen Darmstadt und Wiesbaden, den Schulverwaltungsstandorten Nord (Homberg), Mitte (Friedberg), Süd (Frankfurt), den angegliederten Internaten und Frühberatungsstellen sowie den Stiftungsforsten Kloster Haina.

Die Leitlinie beruht auf akzeptierten Grundprinzipien zum Datenschutz.

Die Wahrung des Datenschutzes ist die Basis für eine vertrauensvolle Zusammenarbeit zwischen dem LWV Hessen, den Leistungsberechtigten, Leistungserbringern und Geschäftspartnern.

Zu unseren Datenschutzzielen gehören:

- die unbedingte Einhaltung der gesetzlichen Vorgaben wie z. B. der EU-DSGVO, des HDSIG, der einschlägigen Regelungen zum Sozialdatenschutz im SGB X etc. durch alle Beschäftigten,
- die unbedingte Einhaltung der internen Datenschutzvorschriften durch alle Beschäftigten,
- die strikte Verpflichtung zur Geheimhaltung und Vertraulichkeit und
- eine datenschutzkonforme Arbeitsplatzgestaltung.

Dabei gelten folgende Grundsätze:

- Die Behördenleitung stellt sicher, dass alle Beschäftigten über diese Leitlinie informiert werden. Das gilt auch für temporär Beschäftigte sowie Auszubildende und Anwärter/innen.
- Alle Führungskräfte und Beschäftigte sind in ihrem Verantwortungsbereich für die Umsetzung und Einhaltung der Leitlinie verantwortlich.

- Die Umsetzung der Leitlinie in den jeweiligen Organisationseinheiten ist Führungsaufgabe.
- Die/Der Datenschutzbeauftragte berät bei der Umsetzung der Leitlinie und prüft deren Einhaltung.

Die aktuelle Version der Datenschutzleitlinie kann auf der Internetseite des LWV Hessen (www.lwv-hessen.de) abgerufen werden.

2. Verantwortlichkeiten

2.1 Behördenleitung

Die Behördenleitung ist für die rechtskonforme Datenverarbeitung verantwortlich. Damit ist sie verpflichtet sicherzustellen, dass die gesetzlichen Anforderungen des Datenschutzes eingehalten werden.

Dies erfolgt durch die Bereitstellung organisatorischer, personeller und technischer Maßnahmen und Vorgaben für eine ordnungsgemäße Datenverarbeitung unter Beachtung des Datenschutzes. Die Behördenleitung hat darüber hinaus sicherzustellen, dass die Beschäftigten im erforderlichen Umfang zum Datenschutz geschult werden. Gleichzeitig ist die Behördenleitung verpflichtet, die/den Datenschutzbeauftragte/n in ihrer/seiner Tätigkeit zu unterstützen.

2.2 Beschäftigte

Die Umsetzung der vorgenannten Vorgaben liegt in der Verantwortung des/der zuständigen Beschäftigten.

Die für Geschäftsprozesse und Projekte fachlich verantwortlichen Beschäftigten informieren die/den Datenschutzbeauftragten rechtzeitig vor Beginn der Verarbeitung über neue Verarbeitungen personenbezogener Daten.

Eine missbräuchliche Verarbeitung personenbezogener Daten oder andere Verstöße gegen das Datenschutzrecht können ggf. zu Meldungen an die Aufsicht führen, die für die/den Betroffenen Bußgelder oder Schadensersatzansprüche nach sich ziehen können. Insofern können Zuwiderhandlungen, für die einzelne Beschäftigte verantwortlich sind, ggf. auch zu arbeits- bzw. dienstrechtlichen Sanktionen führen.

3. Die/Der behördliche Datenschutzbeauftragte

3.1 Grundsatz

Der Landeswohlfahrtsverband Hessen hat nach Maßgabe des § 5 HDSIG i. V. m. Artikel 37 EU-DSGVO eine/n interne/n Datenschutzbeauftragte/n (DSB) sowie eine Stellvertretung benannt.

Die Kontaktdaten der/des Datenschutzbeauftragten lauten:

datschutzbeauftragte@lwv-hessen.de
Datenschutzbeauftragte des LWV Hessen
Stabsstelle 030
Ständeplatz 6 - 10
34117 Kassel

Die/Der Datenschutzbeauftragte ist verantwortlich für die Sicherstellung des Datenschutzes nach der EU-DSGVO (vgl. hierzu Art. 37 - 39 EU-DSGVO), dem Hessischen Datenschutz-

und Informationsfreiheitsgesetz (vgl. hierzu insb. § 7 HDSIG), nach den Datenschutzvorschriften der Sozialgesetzbücher (vgl. hier insb. § 81 Abs. 2 und 4 SGB X) sowie der Dienstanweisung für den/die Datenschutzbeauftragte/n des LWV Hessen als interne Vorschrift (siehe hierzu auch Ziffer 17.3.3.1 des Organisationshandbuches des LWV Hessen).

Der Zuständigkeitsbereich umfasst die Hauptverwaltung Kassel, die Regionalverwaltungen Darmstadt und Wiesbaden, die überregionalen Schulen mit den dort angegliederten sozialen Einrichtungen sowie die Stiftungsforsten Kloster Haina.

Die/Der Datenschutzbeauftragte ist weisungsfrei und als Stabsstelle der/dem Landesdirektorin/Landesdirektor direkt unterstellt.

Die Aufgaben und Pflichten sind intern in der Dienstanweisung für die/den Datenschutzbeauftragte/n des LWV Hessen geregelt (siehe hierzu auch Ziffer 17.3.3.1 des Organisationshandbuches des LWV Hessen).

3.2 Aufgaben

Die/Der Datenschutzbeauftragte unterrichtet und berät die Behördenleitung, die Beschäftigten und auch Externe hinsichtlich ihrer Datenschutzrechte und -pflichten.

Sie/Er überwacht die Einhaltung der einschlägigen Datenschutzgesetze und -vorschriften sowie die Strategien der Behördenleitung für den Schutz der personenbezogenen Daten und für die Sensibilisierung und Schulung der Beschäftigten.

Im Falle risikoreicher Datenverarbeitungen steht die/der Datenschutzbeauftragte der Behördenleitung bzw. der jeweils für die Datenverarbeitung verantwortlichen Organisationseinheit beratend bei der Abschätzung des Risikos und ggf. bei der Durchführung einer Datenschutzfolgenabschätzung zur Seite.

Die/Der Datenschutzbeauftragte berichtet der Behördenleitung alle 2 Jahre in einem Tätigkeitsbericht.

4. Datenschutzkoordinatorinnen und -koordinatoren

Die Behördenleitung kann an einzelnen Verwaltungsstandorten Datenschutzkoordinatorinnen oder -koordinatoren benennen. Diese unterstützen die/den Datenschutzbeauftragte/n bei der

- Ermittlung der für die Verarbeitung von personenbezogenen Daten relevanten Sachverhalte, insbesondere der möglichen technischen und/oder organisatorischen Schwachstellen,
- Kommunikation mit der/dem Datenschutzbeauftragten
- Überwachung der Umsetzung der Datenschutzmaßnahmen im Zuständigkeitsbereich
- Bekanntmachung der Vorgaben und Empfehlungen der/des Datenschutzbeauftragten

5. Datenschutzkontrolle

Die Einhaltung der internen Leitlinien zum Datenschutz und der geltenden Datenschutzgesetze wird durch Datenschutzaudits und weitere Kontrollen überprüft. Die Themen und Prüfzeiträume werden risikoorientiert im Rahmen einer entsprechenden Jahresplanung festgelegt.

Die aus den Prüfungen und Audits resultierenden Ergebnisse sind der Behördenleitung mitzuteilen.

6. Verpflichtung/Schulung der Beschäftigten

Jede/r Beschäftigte, die/der Umgang mit personenbezogenen Daten hat, ist zu einem vertraulichen Umgang mit diesen Daten und auf die Einhaltung dieser Leitlinie verpflichtet.

Die Verpflichtung erfolgt unter Verwendung des hierzu vorgesehenen Formulars und unter Aushändigung des Merkblatts „*MERKBLATT für den Datenschutz bei der Datenverarbeitung im LWV Hessen*“ durch den Fachbereich Personal.

Beschäftigte, die besonderen Geheimhaltungsverpflichtungen unterliegen, werden von den jeweiligen Führungskräften ergänzend über die Einhaltung des Datenschutzes unterrichtet. Diese Erklärungen sind zur Personalakte zu nehmen.

Die/Der Datenschutzbeauftragte wird durch den Fachbereich Personal bzw. die Schulverwaltungsleitungen über Neueinstellungen regelhaft einmal jährlich informiert, um notwendige Datenschutzunterweisungen oder Datenschutzkontrollen zeitlich planen zu können.

Für Beschäftigte, die die unterschiedlichen Formen mobiler Arbeit nutzen, sind regelmäßige Datenschutzunterweisungen verpflichtend.

7. Grundsätze für die Verarbeitung personenbezogener Daten

7.1 Rechtmäßigkeit der Verarbeitung

Bei der Verarbeitung personenbezogener Daten ist das informationelle Selbstbestimmungsrecht des/der Betroffenen zu wahren.

Personenbezogene Daten müssen immer auf rechtmäßige Weise erhoben und verarbeitet werden.

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nur zulässig, wenn einer der nachfolgenden Erlaubnistatbestände vorliegt. Ein solcher Erlaubnistatbestand ist auch dann erforderlich, wenn der Zweck für die Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten gegenüber der ursprünglichen Zweckbestimmung geändert werden soll.

7.1.1 Datenverarbeitung aufgrund rechtlicher Verpflichtung

Die Verarbeitung der personenbezogenen Daten erfolgt aufgrund gesetzlicher Vorschriften.

7.1.2 Einwilligung in die Datenverarbeitung

Die Verarbeitung der personenbezogenen Daten erfolgt aufgrund einer Einwilligung der/des Betroffenen.

Vor der Einwilligung ist die/der Betroffene gemäß dieser Datenschutzleitlinie über die Datenverarbeitung zu informieren. Die Einwilligungserklärung ist aus Gründen der Nachweispflichten der verantwortlichen Stelle grundsätzlich schriftlich einzuholen. Im Einzelfall, z. B. bei telefonischer Beratung, kann die Einwilligung zunächst auch mündlich erteilt werden. Die Erteilung muss dann entsprechend dokumentiert werden; die schriftliche Einwilligung ist nachträglich einzuholen.

7.1.3 Datenverarbeitung für eine vertragliche Beziehung

Wenn die Datenverarbeitung personenbezogener Daten der Vertragserfüllung oder der Erfüllung vorvertraglicher Maßnahmen dient, so ist die Verarbeitung zulässig.

7.1.4 Datenverarbeitung für die Zwecke des Beschäftigungsverhältnisses

Personenbezogene Daten von Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung, Beendigung oder Abwicklung sowie zur Durchführung innerdienstlicher planerischer, organisatorischer, sozialer oder personeller Maßnahmen erforderlich ist.

Bewerberdaten sind nach Ablehnung der Bewerberin/des Bewerbers unter Berücksichtigung beweisrechtlicher Fristen zu löschen, es sei denn, die Bewerberin/der Bewerber hat in eine weitere Speicherung für einen späteren Auswahlprozess eingewilligt. Eine Einwilligung ist auch für eine Verwendung der Daten für weitere Bewerbungsverfahren erforderlich.

Verarbeitungen von personenbezogenen Daten, die zwar im Kontext des Beschäftigungsverhältnisses stehen, jedoch nicht originär der Erfüllung des Arbeitsvertrages dienen, erfordern eine rechtliche Legitimation, wie bspw. gesetzliche Anforderungen, Dienstvereinbarungen (als Kollektivvereinbarungen) oder die Einwilligung der/des Beschäftigten.

Kontrollmaßnahmen, die eine Verarbeitung von Beschäftigtendaten erfordern, dürfen nur durchgeführt werden, wenn dazu eine gesetzliche Verpflichtung besteht, die Maßnahmen in einer Dienstvereinbarung getroffen wurden oder ein begründeter Anlass gegeben ist.

Auch bei Vorliegen eines begründeten Anlasses ist immer vorab die Verhältnismäßigkeit der Kontrollmaßnahme zu prüfen. Die berechtigten Interessen der Behördenleitung an der Durchführung der Kontrollmaßnahme (z. B. Einhaltung rechtlicher Bestimmungen oder interner Regeln) sind immer gegen das schutzwürdige Interesse der/des von der Maßnahme Betroffenen abzuwägen und dürfen nur durchgeführt werden, wenn sie angemessen sind.

Diese Abwägung ist vor jeder Maßnahme durchzuführen und zu dokumentieren.

7.1.5 Verarbeitung besonders schutzwürdiger Daten

Die Verarbeitung besonders schutzwürdiger personenbezogener Daten darf nur erfolgen, wenn dies gesetzlich erforderlich ist oder der/die Betroffene ausdrücklich eingewilligt hat. Die Verarbeitung dieser Daten ist auch dann zulässig, wenn sie zwingend notwendig ist, um rechtliche Ansprüche gegenüber dem/der Betroffenen geltend zu machen, auszuüben oder zu verteidigen.

7.1.6 Datenverarbeitung aufgrund von Kollektivvereinbarungen

Kollektivvereinbarungen wie Tarifverträge einerseits oder Dienstvereinbarungen zwischen Behördenleitung und Personalräten/Gesamtpersonalräten andererseits regeln spezielle Themenbereiche im Rahmen der Möglichkeiten des Beschäftigungsrechts. Die Regelungen müssen sich auf den konkreten Zweck der gewünschten Verarbeitung erstrecken und sind im Rahmen des geltenden Datenschutzrechts gestaltbar.

7.1.7 Datenverarbeitung aufgrund berechtigten Interesses

Die Verarbeitung personenbezogener Daten kann auch erfolgen, wenn dies zur Verwirklichung eines berechtigten Interesses des LWV Hessen erforderlich ist (bspw. Videoüberwachung Tiefgarage). Eine Verarbeitung personenbezogener Daten aufgrund eines berechtigten Interesses darf nicht erfolgen, wenn es im Einzelfall einen Anhaltspunkt dafür gibt, dass schutzwürdige Interessen des/der Betroffenen das Interesse an der Verarbeitung

überwiegen. Eine entsprechende Interessensabwägung hat für jede Verarbeitung zu erfolgen.

7.1.8 Automatisierte Einzelentscheidungen

Automatisierte Verarbeitungen personenbezogener Daten, durch die einzelne Persönlichkeitsmerkmale von Betroffenen bewertet werden, finden beim LWV Hessen nicht statt.

7.2 Zweckbindung

Die Verarbeitung personenbezogener Daten darf lediglich zu dem Zweck erfolgen, der vor der Erhebung der Daten festgelegt wurde. Nachträgliche Änderungen des Zwecks sind nur in Ausnahmefällen möglich und bedürfen einer detaillierten schriftlichen Begründung, welche vorab der/dem Datenschutzbeauftragten zur Stellungnahme zuzuleiten ist.

7.3 Betroffenenrechte

Im Rahmen einer transparenten Datenverarbeitung ist die/der Betroffene beim Erstkontakt über den Umgang mit ihren/seinen Daten zu informieren. Dies erfolgt in den sog. Datenschutzhinweisen, welche der/dem Betroffenen vor Beginn der Verarbeitung übergeben werden und die detailliert Auskunft über die Wahrnehmung der Betroffenenrechte geben.

7.3.1 Recht auf Auskunft

Die/Der Betroffene kann nach Art. 15 EU-DSGVO Auskunft darüber verlangen, welche personenbezogenen Daten welcher Herkunft über sie/ihn zu welchem Zweck gespeichert sind.

Werden personenbezogene Daten an Dritte übermittelt, muss auch über die Identität des Empfängers/der Empfängerin oder über die Kategorien von Empfängern/Empfängerinnen Auskunft gegeben werden.

7.3.2 Recht auf Berichtigung

Sind personenbezogene Daten unrichtig oder unvollständig, kann die/der Betroffene nach Art. 16 EU-DSGVO seine/ihre Berichtigung oder Ergänzung verlangen.

7.3.3 Recht auf Löschung

Die/Der Betroffene ist berechtigt, nach Art. 17 EU-DSGVO die Löschung ihrer/seiner Daten zu verlangen, wenn die Rechtsgrundlage für die Verarbeitung der Daten fehlt oder weggefallen ist. Gleiches gilt für den Fall, dass der Zweck der Datenverarbeitung durch Zeitablauf oder aus anderen Gründen entfallen ist. Bestehende Aufbewahrungspflichten und einer Löschung entgegenstehende schutzwürdige Interessen müssen beachtet werden.

7.3.4 Recht auf Einschränkung der Verarbeitung

Die/Der Betroffene kann eine Einschränkung der Verarbeitung nach Art. 18 EU-DSGVO fordern.

7.3.5 Recht auf Widerspruch

Die/Der Betroffene hat nach Art. 21 EU-DSGVO ein grundsätzliches Widerspruchsrecht gegen die Verarbeitung ihrer/seiner Daten. Dies gilt nicht, wenn eine Rechtsvorschrift zur Durchführung der Verarbeitung verpflichtet.

7.3.6 Recht auf Datenübertragbarkeit

Die/Der Betroffene hat nach Art. 20 EU-DSGVO das Recht zu erwirken, die ihre/seine Person betreffenden Daten, die aufgrund einer Einwilligung oder eines Vertrags erhoben wurden, in einem strukturierten und maschinenlesbaren Format zu erhalten bzw. dass die Daten direkt von einem/einer Verantwortlichen zu einem/einer anderen Verantwortlichen übermittelt werden, soweit dies technisch möglich ist.

Die zentrale Bearbeitung aller vorgenannten Betroffenenrechte erfolgt durch die/den Datenschutzbeauftragte/n. Die zugrunde liegenden Prozesse sind intern in der Geschäftsanweisung Betroffenenrechte und Datenschutzpannen geregelt (siehe hierzu auch Ziffer 4.2.3 des Organisationshandbuches des LWV Hessen).

7.4 Datenvermeidung und Datensparsamkeit

Vor Beginn einer Verarbeitung personenbezogener Daten ist immer zu prüfen, ob und in welchem Umfang diese notwendig ist, um den mit der Verarbeitung angestrebten Zweck zu erreichen. Dabei sind grundsätzlich so wenige Daten wie möglich zu erheben (Minimalprinzip). Die Daten sind zu anonymisieren oder zumindest zu pseudonymisieren, wenn es zur Erreichung des Zwecks möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Zweck steht.

7.5 Aufbewahrungsfristen und Löschung

Personenbezogene Daten, die für den bei der Erhebung festgelegten Zweck nicht mehr benötigt werden, sind zunächst für die gesetzlich vorgeschriebene oder geschäftsprozessbezogene Aufbewahrungsfrist zu archivieren. Damit werden sie dem Zugriff der Sachbearbeitung entzogen. Nach Ablauf dieser Frist sind sie zu löschen. Soweit entsprechende Aufbewahrungsfristen nicht vom Gesetzgeber vorgegeben werden, sind sie in einer internen Richtlinie festgelegt.

Bestehen im Einzelfall Anhaltspunkte für schutzwürdige Interessen oder für eine historische Bedeutung dieser Daten, welche gegen eine Löschung sprechen, ist dies schriftlich zu dokumentieren.

Die Aufbewahrungsfristen beim LWV Hessen sind in der Anlage 7 zur Dienstanweisung für die Schriftgutverwaltung festgeschrieben und werden regelmäßig evaluiert und ggf. angepasst.

7.6 Sachliche Richtigkeit und Datenaktualität

Personenbezogene Daten sind sachlich richtig, vollständig und in der aktuellen Version zu speichern. Hierzu sind angemessene Maßnahmen zu treffen. Sind Daten im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig, sind sie unverzüglich zu löschen oder zu berichtigen.

7.7 Vertraulichkeit

Für personenbezogene Daten gilt das Datengeheimnis. Sie müssen im persönlichen Umgang vertraulich behandelt werden und durch angemessene organisatorische und technische Maßnahmen gegen unberechtigten Zugriff, unrechtmäßige Verarbeitung oder Weitergabe sowie versehentlichen Verlust, Veränderung oder Zerstörung gesichert werden.

Eine unbefugte Erhebung, Verarbeitung oder Nutzung ist den Beschäftigten des LWV Hessen untersagt.

Unbefugt ist jede Verarbeitung, die Beschäftigte vornehmen, ohne damit im Rahmen ihrer zugewiesenen Aufgabenerfüllung betraut und entsprechend berechtigt zu sein.

Um diesen Grundsatz zu erfüllen, erfolgt beim LWV Hessen eine sorgfältige Aufteilung und Trennung von Rollen und Zuständigkeiten sowie deren Umsetzung und Pflege im Rahmen von Berechtigungskonzepten.

Beschäftigte dürfen darüber hinaus dienstliche personenbezogene Daten nicht für eigene private oder wirtschaftliche Zwecke nutzen, an Unbefugte übermitteln oder diesen auf andere Weise zugänglich machen.

7.8 Datensicherheit

Personenbezogene, sensible Daten werden beim LWV Hessen durch die Implementierung unterschiedlicher Sicherheitsmechanismen und -prozesse gegen unberechtigten Zugriff, unrechtmäßige Verarbeitung oder Weitergabe sowie gegen Verlust, Verfälschung oder Zerstörung geschützt. Dies gilt unabhängig davon, ob die Datenverarbeitung elektronisch oder in Papierform erfolgt.

Vor Einführung neuer IT-Verfahren, insb. neuer IT-Systeme, werden technische und organisatorische Maßnahmen zum Schutz der personenbezogenen Daten festgelegt und umgesetzt. Diese Maßnahmen orientieren sich am Stand der Technik, den von der Verarbeitung ausgehenden Risiken und dem Schutzbedarf der Daten (ermittelt durch den Prozess zur Informationsklassifizierung).

Die technisch-organisatorischen Maßnahmen zum Schutz personenbezogener Daten sind Teil des LWV-weiten Informationssicherheits- und Datenschutz-Managements und werden kontinuierlich an die technischen Entwicklungen und die organisatorischen Änderungen angepasst.

Zur Wahrung der Verfügbarkeit, Vertraulichkeit und Integrität der Daten sowie der Belastbarkeit der datenverarbeitenden Systeme ist ein allgemeines Sicherheitskonzept erstellt. Es orientiert sich an der zuvor erstellten Schutzbedarfsfeststellung und der Risikoanalyse.

Weiterhin bestehen ergänzende interne Regelungen, die insb. die im Zusammenhang mit Art. 32 EU-DSGVO zur Realisierung der Datensicherheit notwendigen Maßnahmen betreffen.

7.9 Rechenschafts- und Dokumentationspflichten

Seitens der für die Datenverarbeitung verantwortlichen Stelle sind nach der EU-DSGVO umfangreiche Rechenschafts- und Dokumentationspflichten einzuhalten, um gegenüber der Aufsichtsbehörde nachweisen zu können, dass die Datenschutzvorgaben eingehalten werden. Diese Nachweisbarkeit („Accountability“) erfolgt insb. durch eine schlüssige und nachvollziehbare schriftliche Dokumentation hinsichtlich getroffener Maßnahmen und dazugehöriger Abwägungen.

Folgende Dokumentationen stellen die Basis dar:

- Verzeichnis von Verarbeitungstätigkeiten
- Dokumentation der technisch-organisatorischen Maßnahmen
- Risikoanalyse und ggf. Datenschutzfolgeabschätzung für die Verarbeitungen
- Abschluss und Ablage von Verträgen zur Auftragsverarbeitung
- Datenschutzleitlinie

- Nachweise über die Schulung/Unterweisung der Beschäftigten zum Datenschutz
- Maßnahmen zur Erfüllung der Transparenzpflichten

7.9.1 Verzeichnis der Verarbeitungstätigkeiten und Datenschutzfolgenabschätzung

Für alle Verarbeitungstätigkeiten mit personenbezogenen Daten führt die/der Datenschutzbeauftragte ein Verzeichnis der Verarbeitungstätigkeiten gem. Art. 30 EU-DSGVO. Dieses Verzeichnis wird nach dem intern geltenden Muster von der für die jeweilige Verarbeitung verantwortlichen Stelle erstellt und der/dem Datenschutzbeauftragten vor Einsatz des Verfahrens vorgelegt.

Unabhängig von dieser Meldung wird die/der Datenschutzbeauftragte bei der Planung neuer Verarbeitungen bzw. der Veränderung bestehender Verfahren bereits im Vorfeld informiert. Bei standardisierten Erhebungen (Fragebögen, Auswertungen, Eingabefelder auf der Internet-Homepage etc.) wird der Erhebungsbogen bzw. die Abfragefelder o. Ä. der/dem Datenschutzbeauftragten vor Einsatz zur Stellungnahme vorgelegt.

Soweit die/der Datenschutzbeauftragte feststellt, dass die beabsichtigte Verarbeitung einer Datenschutzfolgenabschätzung unterliegt, teilt sie/er dies der für die Verarbeitung verantwortlichen Stelle umgehend mit. In diesem Fall darf das Verfahren erst nach Erstellung der Datenschutzfolgenabschätzung und der anschließenden Zustimmung der/des Datenschutzbeauftragten in den Echtbetrieb gehen.

7.9.2 Dokumentation der technischen und organisatorischen Maßnahmen

Das Dokument beschreibt die beim LWV Hessen als verbindlich festgelegten technisch-organisatorischen Maßnahmen. Sie gelten für alle Beschäftigten des LWV Hessen sowie auch für Externe im Rahmen ihrer vom LWV Hessen beauftragten Tätigkeiten.

7.9.3 Dokumentation von Anfragen und Anträgen zur Wahrung der Betroffenenrechte

Die zugrunde liegenden Prozesse sind intern in der Geschäftsanweisung Betroffenenrechte und Datenschutzpannen (siehe hierzu auch Ziffer 4.2.3 des Organisationshandbuches des LWV Hessen) geregelt. Die entsprechenden Anfragen und Beschwerden werden durch die Stabsstelle 030 bearbeitet und im Rahmen des Datenschutzmanagements dort verwaltet.

7.9.4 Datenschutzerklärung

Die Datenschutzerklärung auf der Internetseite des LWV Hessen enthält weitergehende Informationen zum Datenschutz wie bspw. zum Umgang mit Cookies.

8. Erhebung/Verarbeitung von personenbezogenen Daten

Die Erhebung und Verarbeitung personenbezogener Daten erfolgt ausschließlich im Rahmen des rechtlich Zulässigen. Hierbei werden auch die besonderen Voraussetzungen für die Erhebung und Verarbeitung sensibler Daten gemäß Art. 9 Abs. 1 EU-DSGVO beachtet. Dabei werden nur solche Informationen verarbeitet und genutzt, die zur direkten Aufgabenerfüllung erforderlich sind und in unmittelbarem Zusammenhang mit dem Verarbeitungszweck stehen.

Die für die Verarbeitung verantwortliche Stelle legt vor der Erhebung bzw. der Speicherung von Daten schriftlich fest, ob und in welcher Art und Weise den gesetzlichen Benachrichtigungspflichten gegenüber den Betroffenen zu genügen ist.

Es ist sichergestellt, dass Betroffene keiner Entscheidung unterworfen werden, die ausschließlich auf einer automatisierten Verarbeitung beruhen und zugleich den Betroffenen gegenüber eine rechtliche Wirkung entfalten oder sie in ähnlicher Weise erheblich beeinträchtigen (bspw. Profiling).

Vor Einführung neuer Datenerhebungen wird die Zulässigkeit durch die für die Datenverarbeitung verantwortliche Stelle in Abstimmung mit der Stabsstelle 030 (Datenschutz und Korruptionsprävention) geprüft. Dies wird zu einem ordnungsgemäßen Nachweis schriftlich dokumentiert.

Eine Zweckänderung ist grundsätzlich nur dann zulässig, wenn die Verarbeitung mit denjenigen Zwecken vereinbar ist, für die die Daten ursprünglich erhoben worden sind. Die im Rahmen der Zweckänderung anzuwendenden Abwägungs-Kriterien werden einzeln geprüft und dokumentiert. Darüber hinaus ist eine Zweckänderung auch dann zulässig, wenn die Einwilligung der betroffenen Person durch die verantwortliche Stelle eingeholt wird.

Falls andere Stellen Informationen über Betroffene anfordern, dürfen diese ohne Einwilligung des/der Betroffenen nur gegeben werden, wenn hierfür eine gesetzliche Verpflichtung oder ein die Weitergabe rechtfertigendes legitimes Interesse besteht und die Identität des/der Anfragenden zweifelsfrei feststeht. Im Zweifel ist die/der Datenschutzbeauftragte zu kontaktieren.

9. Datenhaltung/-löschung

Die Speicherung von Daten erfolgt grundsätzlich nur auf den hierzu zur Verfügung gestellten Netzlaufwerken.

Soweit im Einzelfall aus technischen oder organisatorischen Gründen ein anderer Speicherort erforderlich sein sollte (z. B. Notebook, Desktop-PC), ist der/die jeweilige Benutzer/in für die Durchführung der Datensicherung und die Einhaltung der notwendigen Sicherheitsmaßnahmen zum Schutz der verarbeiteten Daten selbst verantwortlich.

Ist ein Netzzugang möglich (z. B. bei Notebook mit WLAN, Tablet), ist zumindest einmal wöchentlich bzw. im Anschluss an wichtige Eingaben/Änderungen der aktuelle Datenbestand auf das für den/die Benutzer/in vorgesehene Netzlaufwerk zu überspielen. Die gewählten Datensicherungsmaßnahmen sind zu dokumentieren.

Gesetzliche Aufbewahrungsfristen und damit einhergehende Löschungstermine sind von der für die Verarbeitung der Daten fachlich zuständigen Organisationseinheit in ihrer eigenen Verantwortung zu beachten und im Verzeichnis der Verarbeitungstätigkeiten entsprechend zu dokumentieren. Die Vernichtung von Datenträgern mit personenbezogenen Daten erfolgt analog der Papiervernichtung und wird im Rahmen der Auftragsverarbeitung durch einen externen Dienstleister durchgeführt.

Bei der Rücknahme nicht mehr benötigter IT-Komponenten ist der Fachbereich 102 verpflichtet, sämtliche noch darauf befindliche benutzerspezifische Daten vor einer erneuten Weiterverwendung der Komponenten datenschutzkonform zu löschen.

10. Übermittlung personenbezogener Daten

Eine Übermittlung von personenbezogenen Daten an Empfänger/innen außerhalb des LWV Hessen unterliegt den gesetzlichen Zulässigkeitsvoraussetzungen der Verarbeitung personenbezogener Daten und darf ausschließlich verschlüsselt erfolgen. Ein entsprechendes Tool steht den Nutzerinnen und Nutzern zur Verfügung.

Im Falle einer Datenübermittlung von Dritten an den LWV Hessen ist sicherzustellen, dass die Daten ausschließlich für die vorgesehenen Zwecke verwendet werden dürfen.

11. Verarbeitung von personenbezogenen Daten im Auftragsverhältnis

Eine Auftragsverarbeitung liegt vor, wenn ein Auftragnehmer mit der Verarbeitung personenbezogener Daten des LWV Hessen beauftragt wird, ohne dass ihm die Gesamtverantwortung für den zugehörigen Geschäftsprozess übertragen wird. In diesen Fällen ist mit externen Auftragnehmern ein Vertrag über eine Auftragsverarbeitung abzuschließen.

Dabei behält der Auftraggeber die Verantwortung für die korrekte Durchführung der Datenverarbeitung; der Auftragnehmer darf seinerseits die personenbezogenen Daten des LWV Hessen ausschließlich im Rahmen des vertraglich festgelegten Umfangs verarbeiten.

Werden externe Dienstleister mit der Verarbeitung personenbezogener Daten beauftragt, so ist die/der Datenschutzbeauftragte vor der Beauftragung unter Vorlage eines Auftragsvertrags und der zusätzlich notwendigen Informationen (z. B. der technisch-organisatorischen Maßnahmen) gem. Art. 28 EU-DSGVO zu informieren. Unter Abwägung des Risikos der Verarbeitung ist der Dienstleister vor Aufnahme der Vertragsleistung durch die/den Datenschutzbeauftragte/n zu prüfen. Ein LWV-Mustervertrag steht zur Verfügung.

Darüber hinaus haben alle externen Kräfte, die für den LWV Hessen im Rahmen eines Dienstleistungsvertrags tätig werden, das Merkblatt für externe, beim LWV Hessen beschäftigte Personen zu unterschreiben.

12. Datenschutzverstöße

Verstöße gegen die Vorschriften zum Schutz personenbezogener Daten bzw. gegen die Datenschutzleitlinie sind unverzüglich an die/den Datenschutzbeauftragte/n des LWV Hessen zu melden.

Hierzu gehören bspw.:

- eine unrechtmäßige Übermittlung personenbezogener Daten an Dritte,
- ein unrechtmäßiger Zugriff durch Dritte auf personenbezogene Daten,
- oder der Verlust personenbezogener Daten.

Die erforderlichen Prozesse sind in der Geschäftsanweisung Betroffenenrechte und Datenschutzspannen (siehe hierzu auch Ziffer 4.2.3 des Organisationshandbuches des LWV Hessen) geregelt.

13. Beschaffung von Hard- und Software

Die Beschaffung von Hard- und Software erfolgt gem. den LWV-internen Leitlinien.

Bei der Auswahl und Implementierung von Hard- und Software wird das Prinzip von Datenschutz durch Technikgestaltung bzw. durch datenschutzfreundliche Voreinstellungen als ein tragendes Kriterium beachtet und entsprechend dokumentiert.

Soll ein neues Verfahren zur Verarbeitung personenbezogener Daten eingeführt werden, wird die/der Datenschutzbeauftragte rechtzeitig vorab von der anfordernden Stelle informiert (siehe hierzu auch Kap. 17.3.3.1 im Organisationshandbuch des LWV Hessen: Dienstanweisung für den Datenschutzbeauftragten). Darüber hinaus ist die

Dienstvereinbarung zur Durchführung von Beteiligungsverfahren (Kap. 18.15 im Organisationshandbuch des LWV Hessen) zu beachten.

Die Beschaffung bzw. die Übernahme der Software in den Echtbetrieb erfolgt erst nach Eingang der vorgeschriebenen Stellungnahmen.

Die/Der Datenschutzbeauftragte berät dahingehend, ob ggf. im Anschluss an eine Risikoabwägung die Durchführung einer Datenschutzfolgenabschätzung erforderlich ist.

Die dienstliche Nutzung privater Hard- und Software ist grundsätzlich untersagt.

Der Fachbereich Datenverarbeitung führt ein Verzeichnis der verwendeten Anwendungsprogramme. Die/Der Datenschutzbeauftragte erhält darüber bei Bedarf jederzeit Auskunft.

Bei Verdacht des Diebstahls von Hard- und Software, des unbefugten Zugriffs auf personenbezogene Daten, von Sabotage oder Datenpannen sind die Behördenleitung, der Fachbereich Datenverarbeitung sowie die/der Datenschutzbeauftragte unverzüglich zu informieren.

Die jeweilige Vorgehensweise ist in der Geschäftsanweisung Betroffenenrechte und Datenschutzpannen bzw. der Geschäftsanweisung Mitteilung besonderer Vorkommnisse geregelt (siehe hierzu auch Ziffern 4.1.3 und 4.2.3 des Organisationshandbuches des LWV Hessen).

14. Telekommunikation und Internet

Telefonanlagen, E-Mail-Adressen, Intranet und Internet werden im Rahmen der dienstlichen Aufgabenstellung durch die Behördenleitung zur Verfügung gestellt. Sie sind Arbeitsmittel und Ressource und dürfen nur im Rahmen der jeweils geltenden Rechtsvorschriften und der internen Leitlinien genutzt werden.

Eine generelle Überwachung der Telefon- und E-Mail-Kommunikation bzw. der Intranet- und Internetnutzung findet nicht statt. Zur Abwehr von Angriffen auf die IT-Infrastruktur oder auf einzelne Nutzer/innen sind netzwerkseitig Schutzmaßnahmen implementiert worden, die schädigende Inhalte blockieren oder die Muster von Angriffen analysieren. Aus Gründen der Sicherheit und Nachvollziehbarkeit erfolgt eine Protokollierung der jeweiligen Nutzung.

Eine personenbezogene Auswertung dieser Daten ist grundsätzlich nicht erlaubt. Die notwendigen Ausnahmen sind durch entsprechende Dienstvereinbarungen intern festgelegt und dürfen nur unter Wahrung des Verhältnismäßigkeitsprinzips erfolgen. Die Auswertungen dienen nicht der Leistungskontrolle.

15. Inkrafttreten

Diese Leitlinie tritt sofort in Kraft und wird unter Ziffer 4.2.4 Bestandteil des Organisationshandbuchs.

(Selbert)

Landesdirektorin

Abkürzungsverzeichnis

Art.	Artikel
Abs.	Absatz
DSB	Datenschutzbeauftragte/r
EU-DSGVO	Europäische Datenschutzgrundverordnung
Ggf.	gegebenenfalls
HDSIG	Hessisches Datenschutz- und Informationsfreiheitsgesetz
IT	Informationstechnologie
i. V. m.	in Verbindung mit
LWV	Landeswohlfahrtsverband
Pkt.	Punkt
SGB	Sozialgesetzbuch