Dienstanweisung über den Datenschutz und die Informationssicherheit im Ministerium des Innern und für Sport

1	**Anwendungsbereich**
2	**Zweck**
3	**Rechtsgrundlagen**
4	**Datenschutzrechtliche Zuständigkeiten**
4.1	Hausleitung
4.2	Zentralabteilung
4.3	Für IT-Recht zuständiges Referat, Behörden-ISBE
4.4	Sonstige Organisationseinheiten
4.5.	Datenschutzbeauftragte/r des MdI
5	**Zusammenarbeit und gegenseitige Information**
5.1	Allgemeine Regelungen
5.2	Information der/des Datenschutzbeauftragten sowie Beteiligung der/des ISBE des MdI
6	**Besondere Verfahrensbestimmungen**
6.1	Verzeichnis der Verarbeitungstätigkeiten gemäß Artikel 30 DS-GVO
6.2	Verfahren bei Datenschutzverletzungen gemäß Artikeln 33, 34 DS-GVO
6.3	Auftragsverarbeitung nach Artikel 28 DS-GVO
7	**Automatisierte Verfahren**
7.1	Verfahren bei der Inbetriebnahme automatisierter Verfahren
7.2	Protokollierung und Auswertung von Beschäftigtendaten
7.3	Wartung und Fernwartung
8	**Verarbeitung personenbezogener Daten in Hybrid- und Papierakten**
9	**Vernichtung von Schriftgut mit personenbezogenen Daten**
10	**Einsatz privater PCs für dienstliche Zwecke**
11	**In-Kraft-Treten**

1 Anwendungsbereich

Diese Dienstanweisung gilt für die Verarbeitung personenbezogener Daten durch alle Organisationseinheiten des Ministeriums des Innern und für Sport Rheinland-Pfalz (MdI). Regelungen in besonderen Rechtsvorschriften sowie in Dienstvereinbarungen, ergänzende Dienstanweisungen und sonstige Bestimmungen bleiben unberührt. Soweit für die Abteilung 6 besondere Regelungen getroffen worden sind, gehen sie den Bestimmungen dieser Dienstanweisung vor.

2 Zweck

Zweck dieser Dienstanweisung ist es, zu gewährleisten, dass Rechte Betroffener beim Umgang mit ihren personenbezogenen Daten nicht beeinträchtigt werden. Die Regelungen dieser Dienstanweisung sowie die Muster in der Anlage zu dieser Dienstanweisung sollen insbesondere sicherstellen, dass die Pflichten des Verantwortlichen nach der DS-GVO zum materiell-rechtmäßigen Umgang mit personenbezogenen Daten (Datenschutz-Compliance)[1] und zur Gewährleistung der Informationssicherheit (Schutz aller, auch nicht personenbezogener, Daten vor z.B. Manipulation, Verlust oder unberechtigter Kenntnisnahme) erfüllt werden.

3 Rechtsgrundlagen

Seit dem 25. Mai 2018 ist die von der Europäischen Union erlassene DS-GVO für die öffentlichen Stellen des Landes Rheinland-Pfalz unmittelbar anzuwenden. Nahezu zum gleichen Zeitpunkt (6. Mai 2018) war auch die Richtlinie (EU) 2016/680 der Europäischen Union (Richtlinie zum Datenschutz bei Polizei und Justiz) in das Recht der Mitgliedstaaten umzusetzen.

Die DS-GVO hat zu einer neuen Struktur des Datenschutzrechts geführt: *Ergänzend* zur DS-GVO als direkt anwendbares Recht haben die öffentlichen Stellen des Landes Rheinland-Pfalz das neu gefasste Landesdatenschutzgesetz (LDSG) vom 8. Mai

[1] Der Begriff Datenschutz-Compliance meint die "Pflicht zum (materiell-) rechtmäßigen Umgang mit personenbezogenen Daten. Auf der anderen Seite gehört ein datensicherer Umgang (Informationssicherheit) mit personenbezogenen Daten gleichermaßen zum Datenschutz (Kramer/ Meints in: Auernhammer, Kommentar zur DS-GVO, 5. Aufl. 2017, Art. 24, Rz. 3). Vgl. zudem auch die Regelungen in Ziffer 4.2., Abs. 1.

2018 (GVBl. 2018, S. 93, BS 204-1) und – je nach Verwaltungsbereich – weiterhin bereichsspezifische datenschutzrechtliche Vorschriften zu beachten.

Wegen der Strukturveränderungen sind im LDSG nur wenige materielle Kernelemente, wie z.B. die Zulässigkeit der Datenverarbeitung zur Erfüllung der in der Zuständigkeit der öffentlichen Stelle liegenden Aufgaben (§ 3 LDSG) oder zur Zweckbindung (§ 30 LDSG) sowie die meisten der besonderen Verarbeitungen betreffenden Regelungen erhalten geblieben. Anderes, insbesondere in Bezug auf den technischen und organisatorischen Datenschutz oder im Hinblick auf die Auftragsverarbeitung, ergibt sich jedoch aus der DS-GVO *unmittelbar.*

4 Datenschutzrechtliche Zuständigkeiten

4.1 Hausleitung

(1) Die Hausleitung stellt mit Unterstützung der nachfolgend genannten Organisationseinheiten sicher, dass die Verarbeitung personenbezogener Daten im Einklang mit den datenschutzrechtlichen Bestimmungen erfolgt.

(2) Die Hausleitung benennt eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten sowie deren oder dessen Vertreterin oder Vertreter.

4.2 Zentralabteilung

(1) Das für den Bereich der Organisation zuständige Referat veranlasst unter Einbeziehung der Hinweise[2] vom 25. Mai 2018 zur Anpassung und Umsetzung der Datenschutzprozesse an die DS-GVO nebst Anlagen in Abstimmung mit der oder dem Informationssicherheitsbeauftragten (ISBE), der oder dem Datenschutzbeauftragten und den betroffenen Organisationseinheiten geeignete technische[3] und organisatorische[4] Daten-

[2] Die "Hinweise zur Umsetzung der DS-GVO" der Abteilung 1, Referat 314, nebst Anlagen sind mit dem LfDI abgestimmt und u.a. elektronisch verfügbar unter:
[redacted]
[redacted] sowie unter: [redacted]

[3] Technische Maßnahmen sind alle Maßnahmen, die sich in technischer Hinsicht auf den Vorgang der Verarbeitung personenbezogener Daten erstrecken. Dazu gehören insbesondere Maßnahmen wie die Pseudonymisierung, Verschlüsselung oder Passwortsicherung.

[4] Organisatorische Maßnahmen sind Maßnahmen, die sich nicht im engeren Sinne auf den technischen Prozess der Verarbeitung beziehen. Dazu gehören u.a. Mitarbeiterschulungen oder die Bestellung eines Datenschutzbeauftragten.

schutzvorkehrungen nach Artikel 24 Absatz 2 i. V. m. Absatz 1 DS-GVO, um zu verhindern, dass die durch die DS-GVO geschützten personenbezogenen Daten ungewollt abfließen, zerstört oder verändert werden (Informationssicherheit[5]). Betreffen Datenschutz-Anweisungen die Informations- und Kommunikationstechnik, gilt Ziffer 4.3.

(2) Das für den Bereich der Organisation zuständige Referat aktualisiert und meldet gemäß Artikel 37 Absatz 7 DS-GVO die Kontaktdaten der oder des Datenschutzbeauftragten der respektive dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz.

(3) Die Verpflichtung neuer Mitarbeiterinnen und Mitarbeiter auf die Einhaltung des Datenschutzes nach § 8 Abs. 2 LDSG (ehemals „Datengeheimnis“) erfolgt durch das Personalreferat unter Verwendung des als **Anlage 1** beigefügten Vordrucks.

4.3 Informationssicherheitsbeauftragte/r (ISBE)

(1) Die oder der Behörden-ISBE erarbeitet, insbesondere in Abstimmung mit dem für den Bereich IT-Recht zuständigen Referat sowie den zuständigen Fachreferaten interne Anweisungen und Regelungen zum Schutz aller Informationen im technischen und nicht-technischen Bereich auf der Basis des BSI Grundschutzkompendiums mit Ausnahme des Bausteins CON.2 Datenschutz. Sie oder er legt dabei insbesondere für die in allen Organisationseinheiten des MdI (mit Ausnahme der Abteilung 6) eingesetzte Informations- und Kommunikationstechnik sowie für die informationstechnischen Verfahren geeignete technische und organisatorische Maßnahmen zum Schutz der zu verarbeitenden personenbezogenen Daten nach Artikel 24 Absatz 1 sowie Artikel 32 DS-GVO fest.

(2) Hierbei ist der Stand der Technik angemessen zu berücksichtigen. Es bedarf deshalb einer stetigen Anpassung der technischen und organisatorischen Maßnahmen sowie der hierzu erlassenen Anweisungen und Regelungen.

[5] Die Informationssicherheit ist im Kontext des Datenschutzes gemäß Artikel 24 Absatz 2 i. V. m. Absatz 1 DS-GVO durch Umsetzung geeigneter technischer und organisatorischer Maßnahmen zu gewährleisten. Zur Abgrenzung der Begriffe "Informationssicherheit" und "Datenschutz-Compliance" vgl. die Ausführungen zu Ziff. 2 sowie zu Ziff. 4.4, Abs. 1.

4.4 Sonstige Organisationseinheiten

(1) Die Organisationseinheiten des MdI tragen für ihren Zuständigkeitsbereich die Verantwortung für die Beachtung der jeweils maßgeblichen datenschutzrechtlichen Vorschriften (Datenschutz-Compliance[6]).

(2) Sie stellen insbesondere sicher, dass

a. die Rechte der betroffenen Personen, insbesondere nach den Artikeln 16 bis 22 DS-GVO,[7]
b. die Informationspflichten gegenüber betroffenen Personen nach den Artikeln 12 bis 14 DS-GVO,
c. die Regelungen zur Übermittlung personenbezogener Daten in Drittländer oder an internationale Organisationen nach Kapitel V (Artikel 44 bis 50) der DS-GVO und
d. die Regelungen zur Auftragsverarbeitung nach den Artikeln 28, 29 DS-GVO[8]

beachtet werden.

(3) Die Organisationseinheiten sind auch zuständig für

a. die Richtigkeit, Vollständigkeit und Aktualität des Verzeichnisses der Verarbeitungstätigkeiten nach Artikel 30 DS-GVO,
b. die Bearbeitung von Auskunftsersuchen von Bürgerinnen und Bürgern gemäß Artikel 15 DS-GVO,
c. die Durchführung der Datenschutz-Folgenabschätzung nach Artikel 35 DS-GVO; ihnen obliegt dabei auch die Pflicht zur Konsultation der oder des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz nach Artikel 36 Absatz 1 bis 3 DS-GVO bei Datenschutz-Folgenabschätzungen,[9] die ein hohes Risiko für die Verarbeitung personenbezogener Daten ergeben. Ziff. 5.2. bleibt unberührt.

---

[6] Zum Begriff *Datenschutz-Compliance* vgl. Fußnote 1.

[7] *Erläuternde* Hinweise zu allen genannten Vorschriften sowie Muster zur Umsetzung finden sich in den Hinweisen zur Umsetzung der DS-GVO der Abteilung 1, Referat 314. Online verfügbar unter: [redacted] sowie unter: [redacted]
Vgl. auch das Datenschutzhandbuch, Teil D (Serviceteil), Ziff. 4.

[8] Zur *Auftragsverarbeitung* vgl. Datenschutzhandbuch, Teil D (Serviceteil), Ziff. 1, (7.).

[9] Zur *Datenschutzfolgenabschätzung* finden Sie Wissenswertes im Datenschutzhandbuch, Teil D (Serviceteil), Ziff. 1, (9.).

d. Die Organisationseinheiten sind auch zuständig für die Festlegung geeigneter technischer Maßnahmen[10] zum Schutz der zu verarbeitenden personenbezogenen Daten nach Artikel 24 Absatz 2 und Artikel 32 DS-GVO (Informationssicherheit)[11] für die in ihrer Zuständigkeit liegenden automatisierten Fachverfahren in Abstimmung mit dem für IT-Recht zuständigen Referat,

e. die Meldung von Datenschutzverstößen an die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz nach Artikel 33 DS-GVO und die Benachrichtigung betroffener Personen nach Artikel 34 DS-GVO gemäß Ziffer 5.2.

f. die Pflicht zur Konsultation der oder des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz bei Erlass eines Gesetzes oder einer Rechtsverordnung, die die Verarbeitung personenbezogener Daten betrifft, nach Artikel 36 Absatz 4 DS-GVO.

4.5 Datenschutzbeauftragte/r des MdI

Zusätzlich zu den durch Artikel 39 Absatz 1 DS-GVO zugewiesenen Aufgaben nimmt die oder der Datenschutzbeauftragte folgende Aufgaben wahr:

a. Führen des Verzeichnisses der Verarbeitungstätigkeiten gemäß Artikel 30 DS-GVO. Ziffer 4.4., Absatz 3 lit. a. dieser Dienstanweisung bleibt unberührt.

b. Einschätzung zur Meldung von Datenschutzverstößen nach Artikel 33 DS-GVO an die oder den Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz sowie zur Pflicht der Benachrichtigung betroffener Personen nach Artikel 34 DS-GVO gemäß Ziffer 6.2. Absatz 6 dieser Dienstanweisung.

[10] Technische Maßnahmen sind alle Maßnahmen, die sich in technischer Hinsicht auf den Vorgang der Verarbeitung personenbezogener Daten erstrecken. Dazu gehören insbesondere Maßnahmen wie die Pseudonymisierung, Verschlüsselung oder Passwortsicherung.
[11] Zur Definition vgl. Ziff. 4.2.

5 Zusammenarbeit und gegenseitige Information

5.1 Allgemeine Regelungen

(1) Die oder der Datenschutzbeauftragte des MdI wird von allen Organisationseinheiten, den Beschäftigten und der Hausleitung bei der Erfüllung seiner Aufgaben unterstützt. Insbesondere arbeiten das für Organisation sowie das für IT-Recht zuständige Referat sowie die oder der Datenschutzbeauftragte zur Gewährleistung des Datenschutzes vertrauensvoll zusammen und informieren sich gegenseitig.

(2) Die Gewährleistung der Informationssicherheit ist ein fortlaufender Prozess, dessen Umsetzung einen regelmäßigen Austausch betroffener Fachbereiche erfordert. Ein Informationssicherheitsteam (IS-Team MdI), bestehend aus Mitgliedern unterschiedlicher Organisationsbereiche des MdI, unterstützt die oder den ISBE fortlaufend beratend bei der Wahrnehmung ihrer/ seiner Aufgaben.

(3) Jede/r Beschäftigte sowie jede Beamtin und jeder Beamte, die/der von einem Datenschutzverstoß Kenntnis erlangt, kann sich unmittelbar an die oder den Datenschutzbeauftragten des MdI wenden. Die oder der Datenschutzbeauftragte behandelt die Mitteilung vertraulich (vgl. Artikel 38 Absatz 5 DS-GVO).

5.2 Beteiligung der/ des Datenschutzbeauftragten sowie der/ des ISBE des MdI

(1) Die oder der Datenschutzbeauftragte des MdI wird frühzeitig in alle wesentlichen Datenschutzfragen, die die Verarbeitung von personenbezogenen Daten im MdI betreffen, eingebunden.

(2) Die oder der Datenschutzbeauftragte des MdI muss insbesondere in folgenden Fällen informiert werden

a. im Vorfeld des Einsatzes eines neuen automatisierten Fachverfahrens sowie bei einer datenschutzrechtlich relevanten Änderung eines bereits eingesetzten automatisierten Fachverfahrens, mit dem personenbezogene Daten verarbeitet werden,

b. vor der Beschaffung von IT-Hard- oder Software, wenn datenschutzrechtlich bedeutsame Anschaffungen geplant werden,

c. bei Durchführung einer Datenschutz-Folgenabschätzung nach Artikel 35 DS-GVO sowie

d. vor Abschluss eines Vertrages zur Auftragsverarbeitung.

(3) Die Information muss so frühzeitig erfolgen, dass die oder der Datenschutzbeauftragte ihren oder seinen Aufgaben gemäß Artikel 39 Absatz 1 DS-GVO nachkommen kann. Die Information ist zu dokumentieren.

(4) Die oder der ISBE muss in den Fällen der Ziffern 5.2 lit. a, b und d so frühzeitig eingebunden werden, dass die Planung und Umsetzung ggf. neuer oder zu ändernder technischer oder organisatorischer Maßnahmen möglich ist. Die Beteiligung ist zu dokumentieren.

6 Besondere Verfahrensbestimmungen

6.1 Verzeichnis der Verarbeitungstätigkeiten gemäß Artikel 30 DS-GVO[12]

(1) Die oder der Datenschutzbeauftragte des MdI übersendet den Abteilungsleitungen jährlich zum 30. Juni eine Liste der von den zugehörigen Organisationseinheiten gemeldeten Verarbeitungstätigkeiten. Die Abteilungen prüfen die Liste auf Richtigkeit und Vollständigkeit, aktualisieren diese und leiten sie der oder dem Datenschutzbeauftragten zu.

(2) Unabhängig davon melden die Organisationseinheiten der oder dem Datenschutzbeauftragten unaufgefordert die neu aufgenommenen Verarbeitungstätigkeiten sowie wesentliche Änderungen bereits gemeldeter Verarbeitungstätigkeiten. Die Meldung sollte unter Verwendung der dafür vorgesehenen Excel-Tabelle (**Anlage 2**) erfolgen, die - ressortweit harmonisiert - allen Organisationseinheiten des MdI zur Verfügung steht.

6.2 Verfahren bei Datenschutzverletzungen gemäß Artikel 4 Nr. 12, Artikel 33 und 34 DS-GVO

(1) Verletzungen des Schutzes personenbezogener Daten im Sinne von Artikel 4 Nummer 12 DS-GVO können zu einer Meldepflicht an die

[12] Zum *Verzeichnis der Verarbeitungstätigkeiten* vgl. auch das Datenschutzhandbuch, Teil C sowie außerdem Teil D (Serviceteil), Ziff. 1, (8.).

Landesbeauftragte oder den Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz nach Artikel 33 DS-GVO sowie zu einer Pflicht zur Benachrichtigung der betroffenen Personen nach Artikel 34 DS-GVO führen.

(2) Im Fall einer Verletzung des Schutzes personenbezogener Daten im Sinne von Artikel 4 Nummer 12 DS-GVO informiert die jeweilige Organisationseinheit, in deren Zuständigkeitsbereich die Datenschutzverletzung vorgefallen ist, über ihre Abteilungsleitung unverzüglich die Datenschutzbeauftragte oder den Datenschutzbeauftragten des MdI hierüber und beteiligt parallel ggf. weitere betroffene Organisationseinheiten zur Sachverhaltsaufklärung. Zu verwenden ist das Formular gemäß **Anlage 3**.[13]

(3) Die oder der Datenschutzbeauftragte des MdI trifft eine Einschätzung, ob eine Meldepflicht nach Artikel 33 DS-GVO oder eine Benachrichtigungspflicht nach Artikel 34 DS-GVO besteht.

(4) Die für die Verarbeitung zuständige Organisationseinheit entscheidet unter Berücksichtigung der Einschätzung der oder des Datenschutzbeauftragten und unter Beteiligung der für die Bereiche Organisation sowie für IT-Recht zuständigen Referate, ob eine Meldung bzw. Benachrichtigung nach Artikel 33 und 34 DS-GVO zu erfolgen hat. Weicht die Organisationseinheit von der Einschätzung der oder des Datenschutzbeauftragten ab, müssen die maßgeblichen Gründe schriftlich dokumentiert werden. Erfolgt entgegen der Einschätzung der oder des Datenschutzbeauftragten keine Meldung oder Benachrichtigung, werden die Amtschefin oder der Amtschef und die oder der Datenschutzbeauftragte des MdI unter Angabe der wesentlichen Gründe für die abweichende Entscheidung schriftlich informiert. Die oder der Datenschutzbeauftragte sowie die beteiligten Referate erhalten eine Kopie zur Kenntnis.

---

[13] Das Formular dient in einem weiteren Verfahrensschritt auch der Meldung der Datenpanne durch die nach Art. 33 DS-GVO meldepflichtigen Stellen an die Aufsichtsbehörde, also an die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz und die Informationsfreiheit. Vgl. hierzu die nachfolgende Regelung in Ziff. 6.2., Abs. 5 dieser Dienstanweisung. Das Formular ist online verfügbar unter: https://www.datenschutz.rlp.de/de/themenfelder-themen/online-services/meldeformular-datenpanne-art-33-ds-gvo/

(5) Im Falle der Meldepflicht hat die Organisationseinheit der Landesbeauftragten oder dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz unverzüglich, möglichst innerhalb einer Frist von 72 Stunden, den Datenschutzverstoß zu melden. Hierfür ist das Formular in **Anlage 3** zu verwenden. Kann die Meldung innerhalb der Frist nicht vollständig erfolgen, weil noch nicht alle Erkenntnisse zur Datenschutzverletzung vorliegen, muss die Meldung unter Verweis auf die Nachmeldung der noch erforderlichen Angaben erfolgen. Ist eine Meldung innerhalb von 72 Stunden nicht möglich, müssen die Gründe hierfür dokumentiert und die Meldung unverzüglich nachgeholt werden. Die Staatssekretärin oder der Staatssekretär und die oder der Datenschutzbeauftragte des MdI werden über die Meldung informiert.

(6) Im Falle der Pflicht zur Benachrichtigung der betroffenen Personen nach Art. 34 DS-GVO erfolgt diese unverzüglich durch die zuständige Organisationseinheit.

(7) Nach Bekanntwerden des Verstoßes leitet die zuständige Organisationseinheit in Abstimmung mit der oder dem Datenschutzbeauftragten des MdI und ggf. weiteren betroffenen Organisationseinheiten unverzüglich Abhilfemaßnahmen ein.

6.3 Auftragsverarbeitung nach Artikel 28 DS-GVO

Die zuständige Organisationseinheit prüft vor Abschluss eines Vertrages über die Auftragsverarbeitung[14], ob der Auftragsverarbeiter hinreichend Garantien dafür bietet, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DS-GVO und den zu ihrer Ergänzung erlassenen europäischen, bundes- und landesrechtlichen Regelungen erfolgt und der Schutz der Rechte der betroffenen Personen gewährleistet wird. Hierzu lässt sie sich entsprechende Nachweise/Zertifikate vorlegen oder führt Ortsbegehungen durch.

7 Automatisierte Verfahren

7.1 Verfahren bei der Inbetriebnahme automatisierter Verfahren

[14] Zur *Auftragsdatenverarbeitung* vgl. auch das Datenschutzhandbuch, Teil D (Serviceteil), Ziff. 1, (7.).

(1) **Grundsatz:** Bei der Entwicklung eines automatisierten Verfahrens, das im MdI betrieben werden soll, sind die jeweilige Verwaltungsaufgabe, die eingesetzten Programme und Verfahren sowie das Datensicherungskonzept durch die fachlich zuständige Stelle unter Beteiligung der systembetreuenden Stelle, der/ dem ISBE und der/ des Datenschutzbeauftragten des MdI schriftlich zu dokumentieren.

(2) **Beschreibung der Verarbeitungstätigkeit:** In einer Beschreibung der Verarbeitungstätigkeit sind die Art der zur automatisierten Verarbeitung vorgesehenen personenbezogenen Daten sowie die einschlägigen Rechtsgrundlagen zu benennen. Diese muss eine eindeutige Abgrenzung gegenüber anderen Verfahren ermöglichen und im Übrigen die wesentlichen Verfahrensschritte von der Eingabe der Daten bis zu dem Ergebnis der Verarbeitung enthalten. Das Erfordernis der Beschreibung der Verarbeitungstätigkeit ist regelmäßig mit der Erstellung der Übersicht über die Verarbeitungstätigkeit nach Artikel 30 DS-GVO unter Verwendung der dafür nach Ziffer 6.1. dieser Dienstanweisung vorgesehenen musterhaften Excel-Tabelle (**Anlage 2)** erfüllt.

(3) **Programm- und Verfahrenstests:** Programme und Verfahren, die bei der Verarbeitung personenbezogener Daten im MdI eingesetzt werden sollen, sind vor ihrem Einsatz im Echtbetrieb zu testen. Hierbei sind insbesondere folgende Punkte zu prüfen:

- Funktionale Anforderungsmerkmale, Erfüllung des Sollverhaltens wie Korrektheit und Vollständigkeit der Verarbeitung.
- Nicht-funktionale Anforderungsmerkmale wie Sicherheit, die Gebrauchstauglichkeit und Zuverlässigkeit.
- Verhalten im Fehlerfall - ob die Verarbeitung von Fehlersituationen korrekt, d. h. wie definiert, erfolgt.

Entsprechen die Ergebnisse bei den einzelnen Tests regelmäßig dem zuvor schriftlich festgelegten erwarteten Ergebnis, darf das Programm bzw. das Verfahren durch die fachlich zuständige Stelle im Einvernehmen mit der systembetreuenden Stelle und der oder dem Datenschutzbeauftragten des MdI freigegeben werden. Die Programme und Verfahren sowie deren Freigabe sind schriftlich zu dokumentieren. Bei eigenentwickelten Pro-

grammen und Verfahren sind auch die Ergebnisse der einzelnen Tests schriftlich festzuhalten.

(4) **Sicherheitskonzept:** Beim Einsatz automatisierter Verfahren sind die gemäß § 24 Abs. 2 DS-GVO notwendigen Datenschutzvorkehrungen zu treffen. Insoweit hat die fachlich zuständige Stelle unter Beteiligung der systembetreuenden Stelle und der oder des Datenschutzbeauftragten des MdI unter Berücksichtigung der Art der zu schützenden Daten, des etwaigen Missbrauchsrisikos und des entsprechenden Kostenaufwands die erforderlichen Maßnahmen zur Gewährleistung des Datenschutzes und der Informationssicherheit in einem Sicherheitskonzept festzulegen. Soweit die notwendigen Datensicherungsmaßnahmen nicht bereits im Rahmen der Beschreibung der Verarbeitungstätigkeit getroffen wurden, sind ergänzende Festlegungen zu treffen und zu dokumentieren.

(5) **Datenschutz-Folgenabschätzung:** Soweit Verfahren automatisierter Verarbeitungen besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen, ist nach Maßgabe des Artikels 35 der DS-GVO eine Datenschutz-Folgenabschätzung[15] durchzuführen. Zu diesem Zweck sind der oder dem Datenschutzbeauftragten des MdI im Falle einer Beratung nach Artikel 39 Absatz 1 lit. c DS-GVO rechtzeitig alle erforderlichen Unterlagen einschließlich einer entsprechenden Risikoanalyse im Rahmen der Datenschutzfolgenabschätzung zuzuleiten. Die Vorgehensweise soll sich an dem Kurzpapier Nr. 5 der DSK zur Datenschutzfolgeabschätzung (Kurzpapier_Datenschutzfolgeabschaetzung.pdf)[16] orientieren.

7.2 Protokollierung und Auswertung von Beschäftigtendaten

(1) **Zweck und Inhalt der Protokollierung:** Für Zwecke der Datenschutzkontrolle, der Datensicherung und zur Gewährleistung des ordnungsgemäßen Betriebs von DV-Verfahren sind einzelne Aktivitäten der Bediensteten und der eingesetzten Systeme in einem Protokoll festzuhalten. Der Gegenstand und der Umfang der zu protokollierenden Aktivitäten sowie die Aufbewahrungsdauer sind durch die systembetreuende Stelle in Abstimmung mit der fachlich zuständigen Stelle und unter Beteiligung des

[15] Zur *Datenschutzfolgenabschätzung* vgl. das Datenschutzhandbuch, Teil D (Serviceteil), Ziff. 1 (9).
[16] Vgl. Anlage 4.

Personalrates und der oder des Datenschutzbeauftragten des MdI schriftlich festzulegen.

(2) **Überprüfung und Auswertung der protokollierten Daten:** Eine Überprüfung und Auswertung von personenbezogenen Daten in Protokolldateien kann durch die systembetreuende Stelle unter Beteiligung der Personalabteilung sowie des Personalrats und der oder des Datenschutzbeauftragten im Rahmen der in Absatz (1) genannten Zwecke erfolgen. Ist eine sofortige Überprüfung und Auswertung der Daten erforderlich, kann die Beteiligung der Personalabteilung sowie des Personalrats unterbleiben, wenn diese zu unvertretbaren Verzögerungen führen würde. Die Personalabteilung und der Personalrat sind unverzüglich über die Durchführung der Kontrolle und ihr Ergebnis zu unterrichten. Eine Auswertung der Protokolldaten für andere Zwecke, insbesondere zur Durchführung von allgemeinen Leistungs- und Verhaltenskontrollen ist gemäß § 20 Abs. 7 LDSG unzulässig.

7.3 Wartung und Fernwartung

(1) Externe: Soweit Beratungsfirmen oder sonstige Unternehmen im Rahmen der Wartung oder Fernwartung von DV-Geräten Kenntnis von personenbezogenen Daten nehmen können, sind bei Abschluss des entsprechenden Wartungsvertrages die Erfordernisse des Art. 28 DS-GVO ("Auftragsverarbeiter") zu beachten.

(2) Umfang der Wartungsarbeiten: Der Umfang der durchzuführenden Arbeiten ist durch die systembetreuende Stelle unter Beteiligung der fachlich zuständigen Stelle und der oder des Datenschutzbeauftragten des MdI festzulegen. Soweit im Rahmen der Durchführung von Wartungsarbeiten die Möglichkeit des Zugriffs auch auf personenbezogene Daten eröffnet werden muss, sind an den jeweiligen Bediensteten der Wartungsfirma insoweit eine Benutzerkennung und ein Passwort zu vergeben. Durch geeignete Maßnahmen ist sicherzustellen, dass Wartungsarbeiten nur im Einzelfall auf Veranlassung der systembetreuenden Stelle durchgeführt werden und diese den Wartungsvorgang verfolgen und jederzeit abbrechen kann.

(3) Protokollierung: Der Zeitpunkt und die Zeitdauer der Wartungsarbeiten sind in geeigneter Weise (z.B. automatische Protokollierung, Eintrag im Systemlogbuch) zu dokumentieren. Des Weiteren sollen alle wesentlichen Wartungsaktivitäten laufend dokumentiert werden.

(4) Besondere Anforderungen bei der Fernwartung: Die Einrichtung eines Verfahrens zur Fernwartung erfolgt durch die systembetreuende Stelle und dem ISBE in Abstimmung mit der fachlich zuständigen Stelle und der oder dem Datenschutzbeauftragten des MdI. Aufgrund des mit einer Fernwartung einhergehenden hohen Risikos durch Externe ist insbesondere darauf zu achten, dass ein Wartungszugang so gestaltet ist, dass ein Transfer von personenbezogenen oder sensitiven Daten zum Fernwartungsplatz unterbunden ist. Bei der Gestaltung der Fernwartungszugänge sind die Vorgaben des Landesbetriebes Daten und Information zu beachten.

8 Verarbeitung personenbezogener Daten in Hybrid- und Papierakten[17]

(1) **Grundsatz:** Werden personenbezogene Daten in Hybrid- und Papierakten verarbeitet, sind unter Berücksichtigung der Art der zu schützenden Daten, des etwaigen Missbrauchsrisikos und des entsprechenden Aufwands angemessene Maßnahmen gegen eine unbefugte Kenntnisnahme zu treffen. Die sich aus datenschutzrechtlichen Vorschriften ergebenden weitergehenden Erfordernisse bleiben unberührt.

(2) **Aufbewahrung:** Besondere Maßnahmen gegen eine unbefugte Kenntnisnahme (Aufbewahrung der Akten in abschließbaren Schränken, Transport im verschlossenen Umschlag) kommen vor allem beim Umgang mit sensiblen Daten (Personalakten, medizinische Gutachten, Sozialdaten) in Betracht. Für die Dauer der Aufbewahrung von Akten gelten die Bestimmungen über die Rechte der betroffenen Person nach Artikeln 12 bis 22 DS-GVO sowie die Landeseinheitliche Aktenordnung und die Vorschriften des Landesarchivgesetzes.

(3) **Verarbeitung:** Die Verarbeitung von personenbezogenen Daten in Akten ist nur zulässig, soweit dies zur Erfüllung der jeweiligen Verwal-

[17] Hinsichtlich der Verarbeitung personenbezogener Daten im Rahmen der E-Akte wird auf die "Dienstvereinbarung über den Einsatz der elektronischen Aktenführung und Vorgangsbearbeitung" vom 24. September 2018 verwiesen.

tungsaufgabe erforderlich ist. Insoweit hat die fachlich zuständige Stelle sicherzustellen, dass bei der Nutzung, Übermittlung und sonstigen Verarbeitung personenbezogener Daten insbesondere die Rechte der betroffenen Person nach Artikeln 12 bis 22 DS-GVO beachtet werden.

(4) **Transport:** Um sicherzustellen, dass personenbezogene Daten beim Transport von Akten nicht unbefugt zur Kenntnis genommen werden können, soll die Versendung an Stellen außerhalb des MdI grundsätzlich in einem verschlossenen Umschlag erfolgen. Eine offene Versendung von Akten mit personenbezogenen Daten an Dritte ist ausnahmsweise zulässig, wenn dies unter Berücksichtigung der Art der personenbezogenen Daten, des Missbrauchsrisikos und des entsprechenden Kostenaufwands ausreichend erscheint.

9 Vernichtung von Schriftgut mit personenbezogenen Daten

(1) **Sammlung des Schriftguts:** Das zur Vernichtung vorgesehene Schriftgut mit personenbezogenen Daten ist von den Mitarbeiterinnen und Mitarbeitern am Arbeitsplatz im Papierkorb zu sammeln. Die entsprechenden Behältnisse werden vom Reinigungspersonal geleert und einem abgeschlossenen Container gesammelt.

(2) **Vernichtung von Schriftgut:** Das im Container gesammelte Schriftgut wird regelmäßig durch ein Datenträgervernichtungsunternehmen abgeholt und unter Berücksichtigung der datenschutzrechtlichen Anforderungen einer Wiederverwertung zugeführt.

(3) **Vernichtung am Arbeitsplatz:** Schriftgut mit besonders schutzwürdigen personenbezogenen Daten soll durch die Bediensteten selbst in den hierfür bereitgestellten Geräten vernichtet werden.

10. Einsatz privater PCs für dienstliche Zwecke

(1) **Grundsatz:** Die Verarbeitung personenbezogener Daten für dienstliche Zwecke auf privaten PCs ist grundsätzlich nicht zulässig. Ausnahmen von diesem Verbot können von der fachlich zuständigen Stelle unter Beteiligung der systembetreuenden Stelle und der oder des Datenschutzbeauftragten des MdI erteilt werden, wenn dienstliche Gründe dies rechtfertigen.

(2) **Besondere Erfordernisse:** Die Erlaubnis zur Nutzung privater PCs für dienstliche Zwecke kann erteilt werden, wenn die oder der jeweilige Bedienstete sich schriftlich verpflichtet,

a. sich der Kontrolle durch die oder den LfDI zu unterwerfen,
b. die Bestimmungen der DS-GVO, des LDSG und die sonstigen Rechtsvorschriften über den Datenschutz zu beachten und
c. lediglich Geräte und Programme einzusetzen, deren Einsatz von der Dienststelle ausdrücklich genehmigt worden ist.

11 In-Kraft-Treten

Diese Dienstanweisung tritt mit Wirkung vom 23. März 2020 in Kraft. Gleichzeitig tritt die Dienstanweisung über den Datenschutz und die Informationssicherheit vom 16. Dezember 2002 außer Kraft.