Erfassung einer Verarbeitungstätigkeit

(bitte an den Datenschutzbeauftragten übersenden)
Nur auszufüllen, wenn personenbezogene Daten (Hinweis Nr. 1) verarbeitet werden!
Anmerkung: Soweit der Platz dieses Formulars nicht ausreicht fügen Sie bitte zusätzliche Anlagen bei.

Datum:	25.05.2018
Ausfüllende Person:	Stefanie Schneider
Telefonnummer:	038828/3301303

Bezeichnung der Verarbeitung (Hinweis Nr. 2): Abruf personenbezogener Daten und verfahrensbedingter Hinweise aus dem Melderegister durch Behörden im verwaltungsinternen Intranet
Übergeordneter Geschäftsprozess: Datenübermittlung an Behörden und sonstige öffentliche Stellen innerhalb derselben Verwaltungseinheit, der auch die Meldebehörde angehört
Beginn der Verarbeitung (Hinweis Nr. 3): laufender Betrieb

☒ **Änderung bestehende Verarbeitung**
☐ **neue Verarbeitung**
☐ **Abmeldung bestehende Verarbeitung (Hinweis Nr. 4)**

1. Grundsätzliche Angaben zur Verarbeitung und zur Verantwortlichkeit.

1.1	Bezeichnung des Verfahrens:	Intranetauskunft MIA (Meldebehördliche Intranet Auskunft) in der jeweils aktuellen Version (Hinweis Nr. 5)
1.2	Fachbereich:	III
	Verantwortliche Führungskraft:	Volker Schuhr
	ggf. Stellen-Kennzeichen:	< Text >
1.3	Ansprechpartner, sofern nicht verantwortliche Führungskraft:	Anja Surkamp
	Telefon-Nummer:	038828/3301310
1.4	Name u. Anschrift des Auftragnehmers, wenn Auftragsverarbeitung nach Art. 28 DSG-VO (Hinweis Nr. 6):	HSH Soft- und Hardware Vertriebs GmbH, Rudolf-Diesel-Str. 2 in 16356 Ahrensfelde bei der Einrichtung des Verfahrens und bei anwendungsbezogenen Fehlerbehebungen (auch im laufenden Betrieb mittels Fernwar-

Vertrags-Nummer: 05-M-011_MVP/15430702M , Vertrag zur Auftragsverarbeitung vom 17.06.2002 – Bestandteil des Hauptvertrages – Installation der MIA Anfang 2005

2. Zweckbestimmung und Rechtsgrundlage der Datenverarbeitung (Hinweis Nr. 7)

2.1 Zweckbestimmung und Rechtsgrundlage der Datenverarbeitung (Hinweis Nr. 8):

Abruf und automatisierter Abruf von Daten aus dem Melderegister durch Behörden und öffentliche Stellen innerhalb einer Verwaltungseinheit, um die vorgeschriebene Aufgabenerfüllung wahrnehmen zu können

2.2 Rechtsgrundlage (zutreffende bitte ankreuzen und erläutern)

☒ Spezialgesetzliche Regelung außerhalb der DSG-VO
(Bitte benennen: Vorschrift, Paragraph, Absatz, Satz)
Bundesmeldegesetz, Ausführungsgesetze zum Bundesmeldegesetz der Länder, Meldeverordnungen bzw. Meldedatenübermittlungsverordnungen, Verwaltungsvorschriften

☐ Einwilligung des Betroffenen (Art. 6 Abs. 1 a) DSG-VO): Bitte fügen Sie die Einwilligungsklausel und den Einwilligungsmechanismus hier ein

< Text >

☐ Kollektivvereinbarung (z.B. Betriebsvereinbarung, Tarifvertrag):
(Bitte benennen: Genaue Bezeichnung, Paragraph, ggfs. Absatz)
< Text >

☐ Begründung, Durchführung oder die Beendigung eines Beschäftigungsverhältnisses (national geregelt im BDSG)
< Text >

☐ Vertrag oder Vertragsanbahnung mit dem Betroffenen
(Art. 6 Abs. 1 b) DSG-VO.)
< Text >

☐ Interessenabwägung (Art. 6 Abs. 1 f) DSG-VO):
Bitte benennen Sie die vorrangigen Interessen
< Text >

3. Kreis der betroffenen Personengruppen

Kreis der betroffenen Personengruppen (Hinweis Nr. 9)	**Art der Daten / Datenkategorien** (Hinweis Nr. 10)	**Werden besonderen Kategorien von Daten verarbeitet?** (Hinweis Nr. 11)	
Alle im Zuständigkeitsbereich der Meldebehörde wohnhaften und wohnhaft gewesenen Personen und deren Lichtbildinformationen aus dem Pass- und Ausweisregister, sofern diese vorliegen	Siehe ***Anlage 1*** für die bundeseinheitlich zu erhebenden Daten	☒ Ja Welche: Religionszugehörigkeit)	☐ Nein

4. Datenweitergabe und deren Empfänger (Hinweis Nr. 12)

4.1 Interne Empfänger innerhalb der verantwortlichen Stelle

Interne Stelle (Org-Einheit)	Behörden und andere öffentliche Stellen in derselben Verwaltungseinheit, der auch die Meldebehörde angehört
Art der Daten	erforderliche und gesetzlich zugelassene Daten aus dem Melderegister und ggfs. aus dem Ausweis- und Passregister
Zweck der Daten-Mitteilung	zur Erfüllung der den abrufenden Stellen übertragenen Aufgaben

4.2 Externe Empfänger und Dritte (jeder andere Empfänger, auch Konzernunternehmen)

Externe Stelle	keine
Art der Daten	entfällt
Zweck der Daten-Mitteilung	entfällt

4.3 Geplante Datenübermittlung in Drittstaaten (außerhalb der EU)

Welcher Staat	keine
Art der Daten	keine
Zweck der Daten-Mitteilung	keine

5. Regelfristen für die Löschung der Daten (Hinweis Nr. 13)

Existieren gesetzliche Aufbewahrungsvorschriften oder sonstige einschlägige Löschungsfristen?

☒ Ja, falls ausgewählt bitte benennen: für die Daten des Melderegister gelten die Bestimmungen der §§ 13 bis 15 BMG, Löschungen in der Intranetauskunft erfolgen nicht, da kein ändernder Zugriff möglich ist

☐ Nein

Bitte beschreiben Sie, ob und nach welchen Regeln die Daten gelöscht werden:

Die Löschung (und ggfs. Archivierung) erfolgt sowohl automatisiert durch die Implementierung der entsprechenden IRIS-Aufgaben zum Löschen und Bereinigen von Registerdaten als auch durch manuelle Betätigung entsprechender Löschungsfunktionalitäten im Melderegister.

6. Mittel der Verarbeitung

Welche Software oder Systeme werden für diese Verarbeitung eingesetzt?

Bezeichnung	Hersteller	Funktionsbeschreibung	Bereitstellung
Intranetauskunft (MIA)	HSH Soft- und Hardware Vertriebs GmbH	Fachverfahren zum Abruf von Daten des Melderegisters und ggfs. Pass- und Ausweisregisters	☐ Eigenentwickelte / Individual Software ☒ Standard- bzw. Kauf-Software ☐ Cloud-Services

7. Zugriffsberechtigte Personengruppen (vereinfachtes Berechtigungskonzept) (Hinweis Nr. 14)

Benennung Personengruppen	Berechtigungsrolle	Umfang des Datenzugriffs (Nennung der Datenarten)	Art des Zugriffs	Zweck des Datenzugriffs
Administrator	Administrator	Personenbezogene Daten, Rechtevergabe an Benutzer	☒ Lesen ☒ Schreiben ☒ Löschen	Benutzerverwaltung
Sachbearbeiter	Benutzer	Personenbezogene Daten	☒ Lesen ☐ Schreiben ☐ Löschen	Personenrecherche
< Text >	< Text >	< Text >	☐ Lesen ☐ Schreiben ☐ Löschen	< Text >

Bitte erläutern Sie kurz den Prozess zur Erlangung und Verwaltung der Berechtigungen oder benennen Sie das detaillierte betriebliche Berechtigungskonzept:
< Text > (ggf. als Anlage anfügen)

8. Technische und organisatorische Maßnahmen (Art. 32 DSGVO) (Hinweis Nr. 15)

8.1 Hinsichtlich der Datensicherheitsmaßnahmen wurde der Bereich IT-Sicherheit eingebunden

☒ Ja
☐ Nein, falls ausgewählt bitte kurze Begründung: < Text >

8.2 Es wurde eine Risikoanalyse gemäß Art. 32 DS-GVO durchgeführt.

☒ Ja
☐ Nein

8.3 Die Maßnahmen des allgemeinen Unternehmens-IT-Sicherheitskonzepts sind den festgestellten Risiken angemessen.

☒ Ja
☐ Nein

8.4 Bitte Angaben zu den abweichenden, bzw. zusätzlichen Maßnahmen ergänzen:
< Text >

Verfügbarkeit	Personenbezogene Daten stehen bei berechtigtem Bedarf zeitnah zur Verfügung um ordnungsgemäß und gesetzkonform ausgewertet bzw. verarbeitet werden zu können: Die Daten einer Person können in der MIA schnell über Suchfunktionen (z.B. über Suche nach Geburtsdatum, Vor- oder Familiennamen) aufgerufen werden und stehen dann für den berechtigten Bearbeiter sofort zur Verfügung. Für Havariefälle hat die Behörde die Möglichkeit, entsprechende Sicherheitssysteme einzusetzen (Parallelsysteme, Datensicherungsmanagement) die eine zeitnahe Weiterarbeit ermöglichen.
Integrität	Personenbezogene Daten bleiben während der Verarbeitung unversehrt, vollständig und aktuell und können nicht verändert werden.

	Natürlich wird der Test der Software als ein integraler Bestandteil der Entwicklung gesehen.
Vertraulichkeit	Personenbezogene Daten sind nur befugten Personen zugänglich: Die MIA ist passwortgeschützt. Jeder berechtigte Mitarbeiter einer Behörde (namentlich benannt) muss sich mit einem eindeutigen Benutzernamen und Passwort exklusiv anmelden. Im Programm kann er dann mit ihm zugeteilten individuell spezifizierten Benutzer-Rechten auf personenbezogene Daten zugreifen. Darüber hinaus sind durch die IT- und DS-Beauftragten der jeweiligen Behörde spezielle organisatorische Maßnahmen zu ergreifen wie z.B. Zugriffsrechte auf Rechner, Verzeichnisse und Dateien sowie Passwortpflege und automatische Bildschirmdeaktivierung.
Weiterer Schutz der Rechte und Freiheiten der Betroffenen	**Authentizität:** Der Abruf personenbezogene Daten kann jederzeit ihrem Ursprung zugeordnet werden: Innerhalb der Software werden alle Zugriffe hinsichtlich des abrufenden Mitarbeiters, des Zeitpunktes und ggfs. des Zwecks des Abrufes protokolliert. Bei Bedarf ist es möglich zusätzliche Verweise auf die Erforderlichkeit eines Datenabrufes zu speichern. **Revisionsfähigkeit:** Durch Beauftragte kann jederzeit festgestellt werden, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet (hier: abgerufen) hat. Alle Vorgänge (hier: Abrufe), die von Programmnutzern einer Behörde an personenbezogene Daten getätigt wurden, werden von der MIA intern mit Benutzernamen und Zeitstempel protokolliert und lassen sich später von hierzu berechtigten Personen über eine Controllingfunktion jederzeit einsehen bzw. auswerten.

Transparenz:

Es ist sichergestellt, dass die Verfahrensweisen bei der Verarbeitung (hier: Abrufe) personenbezogener Daten vollständig und aktuell sind und derart dokumentiert werden, dass sie in angemessener Zeit nachvollziehbar sind:
Jeder Vorgang der sich auf die Verarbeitung (hier: Abrufe) personenbezogener Daten bezieht, wird von der MIA protokolliert und lässt sich in der Fachanwendung schnell nachvollziehen.

9. Datenübertragbarkeit (Hinweis 16)

Ist der Export der verarbeiteten Daten an den Betroffenen oder andere Dienste in einem gängigen, standardisierten Format möglich?

☒ Ja,
☐ Nein

10. Information der Betroffenen (Hinweis 17)

Wie und wo werden den Betroffenen, deren Daten verarbeitet werden, die Pflichtinformationen über die Datenverarbeitung zugänglich gemacht?
entfällt

11. Datenschutz durch Technikgestaltung und Voreinstellungen (Hinweis 18)

Sind bei der Verarbeitung die Grundsätze des Datenschutz durch Technikgestaltung und der datenschutzfreundlichen Voreinstellungen eingehalten?

☒ Ja
☐ Nein

Anmerkungen:
Hinsichtlich einer Benutzerkontrolle ist die MIA mit Login und Passwort geschützt. Jeder Anwender muss sich mit seiner Benutzerkennung und Passwort anmelden und kann erst dann und nur mit den Ihm zugeteilten Benutzerrechten auf die entsprechenden Daten des jeweiligen Registers zugreifen.
Hinsichtlich der Zugriffskontrolle werden in der MIA unterschiedliche Nutzer oder Nutzergruppen mit unterschiedlichen Berechtigungen angelegt, um eine individuelle und differenzierte Rechteverwaltung aufzubauen.
Die Verantwortlichkeits- und Dokumentationskontrolle wird in den Fachanwendungen Meso und VOIS|MESO erreicht, in dem von den Nutzern (auch Administratoren) alle Verarbeitungsvorgänge (hier: Abrufe) mit den jeweiligen Benut-

zernamen und einem Zeitstempel protokolliert werden. Diese Protokolldaten lassen sich jederzeit auswerten.
Über die IRIS im Verfahren Meso bzw. VOIS|MESO (also das Melderegister) die Aufgabenverwaltung im Verfahren VOIS|MESO werden die für die jeweiligen Register erforderlichen Aufgaben einschließlich der Löschung erforderlicher Daten automatisiert und zu jeweils einzeln konfigurierbaren Zeiten, Zeiträumen bzw. Zeitpunkten erledigt.

Anlage 1 – zu laufende Nummer 3: Kreis der betroffenen Personengruppe

Melderegister (incl. Wahlkomponente):

- Familienname,
- frühere Namen,
- Vornamen unter Kennzeichnung des gebräuchlichen Vornamens,
- Doktorgrad,
- Ordens- und Künstlernamen,
- Tag und Ort der Geburt bei Geburt im Ausland auch den Staat,
- Geschlecht,
- gesetzlicher Vertreter (Vor- und Familiennamen, Doktorgrad, Anschrift, Tag der Geburt, Geschlecht, Sterbetag, Auskunftssperren gemäß § 51 BMG),
- derzeitige Staatsangehörigkeiten,
- rechtliche Zugehörigkeit zu einer öffentlich-rechtlichen Religionsgesellschaft,
- derzeitige Anschriften, frühere Anschriften im Zuständigkeitsbereich der Meldebehörde sowie Anschrift der letzten alleinigen Wohnung oder Hauptwohnung und der letzten Nebenwohnung außerhalb des Zuständigkeitsbereichs der Meldebehörde, gekennzeichnet nach Haupt- und Nebenwohnung, bei Zuzug aus dem Ausland auch den Staat und die letzte Anschrift im Inland, bei Wegzug ins Ausland auch die Zuzugsanschrift im Ausland und den Staat,
- Einzugsdatum, Auszugsdatum, Datum des letzten Wegzugs aus einer Wohnung im Inland sowie Datum des letzten Zuzugs aus dem Ausland,
- Familienstand, bei Verheirateten oder Lebenspartnern zusätzlich Tag und Ort der Eheschließung oder der Begründung der Lebenspartnerschaft, sowie bei Eheschließung oder Begründung einer Lebenspartnerschaft im Ausland auch den Staat,
- Ehegatte oder Lebenspartner (Vor- und Familiennamen, Geburtsname, Doktorgrad, Tag der Geburt, Geschlecht, Anschrift, Sterbetag, Auskunftssperren gemäß § 51 BMG),
- minderjährige Kinder (Vor- und Familiennamen, Tag der Geburt, Geschlecht, Anschrift, Sterbetag, Auskunftssperren gemäß § 51 BMG),
- Ausstellungsbehörde, -datum, Gültigkeitsdauer und Seriennummer des gültigen Personalausweises/Passes,
- Tatsache des Vorliegens eines bedingten Sperrvermerks
- Tatsache des Vorliegens einer Auskunftssperre und deren Art, Dauer und ausstellender Behörde
- Tatsache des Vorliegens einer Übermittlungssperre und deren Art
- Sterbetag und –ort, bei Versterben im Ausland auch den Staat.

(2) Über die in Absatz 1 genannten Daten hinaus speichern die Meldebehörden im Melderegister folgende Daten einschließlich der zum Nachweis ihrer Richtigkeit erforderlichen Hinweise:

- für die Vorbereitung und Durchführung von Wahlen und Abstimmungen auf staatlicher und kommunaler Ebene die Tatsache, dass die betroffene Person
- von der Wahlberechtigung oder der Wählbarkeit ausgeschlossen ist,
- als Unionsbürger (§ 6 Abs. 3 Satz 1 des Europawahlgesetzes) bei der Wahl des Europäischen Parlaments von Amts wegen in ein Wählerverzeichnis im Inland einzutragen ist; ebenfalls zu speichern ist die Gebietskörperschaft oder der Wahlkreis im Herkunftsmitgliedstaat, wo er zuletzt in ein Wählerverzeichnis eingetragen war,

- für die Ausstellung von Personalausweisen und Pässen die Tatsache, dass Passversagungsgründe vorliegen, ein Pass versagt oder entzogen oder eine Anordnung nach § 6 Abs. 7 des Personalausweisgesetzes getroffen worden ist,
- für das waffenrechtliche Verfahren die Tatsache, dass eine waffenrechtliche Erlaubnis erteilt worden ist, und die diese Tatsache mitteilende Behörde mit Angabe des Tages der erstmaligen Erteilung,
- für sprengstoffrechtliche Verfahren die Tatsache, dass eine sprengstoffrechtliche Erlaubnis oder ein Befähigungsschein nach § 20 des Sprengstoffgesetzes erteilt worden ist sowie die Behörde, die diese Tatsache mitteilt, mit Angabe des Datums der erstmaligen Erteilung
- für die Prüfung, ob die von der meldepflichtigen Person gemachten Angaben richtig sind, und zur Gewährleistung der Auskunftsrechte in § 19 Absatz 1 Satz 3 BMG und § 50 Absatz 4 BMG den Namen und die Anschrift des Eigentümers der Wohnung und, wenn dieser nicht selbst Wohnungsgeber ist, auch den Namen und die Anschrift des Wohnungsgebers
- für das Verfahren zur Bildung und Anwendung der elektronischen Lohnsteuerabzugsmerkmale nach § 39e Absatz 2 Satz 2 und 3 des Einkommensteuergesetzes
- verfahrensbedingte Hinweise

Pass- und Ausweisregister:

- Lichtbild,
- Unterschrift,
- Seriennummer,

Erläuterungen

Hinweis Nr. 1

»Personenbezogene Daten« sind nach Art. 4 Nr.1 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden »betroffene Person«) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, Dies umfasst z. B. Name, Geburtsdatum, Anschrift, Einkommen, Beruf, Kfz-Kennzeichen, Konto-oder Versicherungsnummer. Auch pseudonymisierte Daten, zum Beispiel eine IP-Adresse oder Personalnummer, aus denen die betroffene Person indirekt bestimmbar wird, gelten als personenbezogener Daten.

Hinweis Nr. 2

Betriebsinterne Benennung, die Identifikation der einzelnen Verarbeitung ermöglicht unter Zuordnung zum jeweiligen Geschäftsprozess, in dem die Daten verarbeitet werden.

Hinweis Nr. 3

Geplanter Beginn der Verarbeitung von personenbezogenen Daten oder tatsächlicher Beginn. Dabei ist schon die erstmalige Übertragung oder Speicherung von Daten relevant.

Hinweis Nr. 4

Nur bei Beendigung der Verarbeitung auszuwählen. Bei Auswahl kann das ursprüngliche Erfassungsformular verwendet werden. In Abstimmung mit dem Datenschutzbeauftragten ist über die weitere Verwendung des Datenbestands zu entscheiden, also ob Löschung oder Migration in andere Verfahren erforderlich ist.

Hinweis Nr. 5

Genaue Kennzeichnung der Verarbeitung mit Mitteln des allgemeinen Sprachgebrauchs und Hinweisen zur Verarbeitung personenbezogener Daten.

Hinweis Nr. 6

Dient der Sicherstellung einer sorgfältigen Auswahl des Dienstleisters, dem Nachweis eines Vertrags und der Wahrnehmung der Kontrollpflichten.

Hinweis Nr. 7

Zieldefinition der Verarbeitung personenbezogener Daten und Nennung der darauf gerichteten rechtlichen Grundlage (Prinzip des Verarbeitungsverbots mit Erlaubnisvorbehalt).

Hinweis Nr. 8

Konkrete Beschreibung des Zwecks der Datenverarbeitung und der Datenverarbeitung selbst. Es empfiehlt sich, entsprechende Erläuterungen möglichst unter der im Unternehmen bekannten Terminologie zu formulieren und in Zweifelsfällen Rücksprache mit dem Datenschutzbeauftragten zu halten.

Hinweis Nr. 9

Nennung der durch die Verarbeitung betroffenen Personengruppen, z. B. Beschäftigte (Mitarbeiter(-gruppen)), Berater, Kunden, Lieferanten, Patienten, Schuldner, Versicherungsnehmer, Interessenten.

Hinweis Nr. 10

Beispiele für Datenkategorien: Identifikations- und Adressdaten, Vertragsstammdaten, Daten zu Bank- oder Kreditkartenkonten, IT-Nutzungsdaten (z. B. Verbindungsdaten, Logging-Informationen).

Hinweis Nr. 11

Die Verarbeitung besonderer Kategorien personenbezogener Daten ist in Art. 9 Abs. 1 DS-GVO geregelt. Umfasst sind Verarbeitungen von Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

Hinweis Nr. 12

Zweck und Empfänger personenbezogener Daten zur Weiterverarbeitung bzw. Nutzung innerhalb der verantwortlichen Stelle oder im Rahmen einer Übermittlung an Dritte.

»Empfänger« ist jede Person oder Stelle, die Daten erhält, z. B. Vertragspartner, Kunden, Behörden, Versicherungen, ärztliches Personal, Auftragsverarbeiter (z. B. Dienstleistungsrechenzentrum, Call-Center, Datenvernichter), oder ein Verfahren, bzw. Geschäftsprozess, an den Daten weitergegeben werden.

Die Art der Daten oder Datenkategorien ist getrennt nach dem jeweiligen Drittstaat und den jeweiligen Empfängern oder Kategorien von Empfängern anzugeben.

Hinweis Nr. 13

Gemäß Art. 5 Abs. 1 e) DS-GVO dürfen personenbezogene Daten nur so lange gespeichert werden, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Unter Beachtung (z.B. steuer-) gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsfristen müssen die Daten nach Zweckfortfall unverzüglich gelöscht werden. Wird keine Löschung ausgewählt oder bei Zweifeln zu Aufbewahrungsfristen und Löschroutinen ist Rücksprache mit dem betrieblichen Datenschutzbeauftragten zu halten.

Hinweis Nr. 14

Skizzierung des Berechtigungsverfahrens und Nennung der berechtigten Gruppen. Sofern vorhanden kann auf ein umfassendes betriebliches Berechtigungskonzept verwiesen werden.

Hinweis Nr. 15

Beschreibung der Schutzmaßnahmen im Hinblick auf die Kontrollziele für die jeweils verarbeiteten personenbezogenen Daten. Im Fall einer festgelegten betrieblichen Sicherheitspolitik im Unternehmen kann der Hinweis auf die Abstimmung mit der Organisationseinheit »IT-Sicherheit« erfolgen.

Ergänzend kann auf die ISO 27001 Bezug genommen werden. Die angegebenen Kontrollziele zur angemessenen Sicherung der Daten vor Missbrauch und Verlust sind dabei nicht abschließender Maßnahmenkatalog zu sehen. So könnten aufgrund des festgestellten besonderen Risikos der Verarbeitung oder einer Spezialgesetzgebung zum Datenschutz weitere Kontrollziele und entsprechende Maßnahmen gefordert sein (z. B. aus dem Telekommunikationsgesetz, aus der Sozialgesetzgebung, oder aus den Landesdatenschutzgesetzen).

Hinweis Nr. 16

Bei Verarbeitungen auf Grundlage eines Vertrages oder einer Einwilligung, für die die Betroffenen dem Unternehmen Daten bereitgestellt haben, haben sie nach Art. 20 DS-GVO das Recht, diese sie betreffenden personenbezogenen Daten, in einem struk-turierten, gängigen und maschinenlesbaren Format zu erhalten oder sie an einen anderen Verantwortlichen übermitteln zu lassen, sofern dies technisch machbar ist.

Hinweis Nr. 17

Nach Art. 12 der DS-GVO müssen beim Verantwortlichen geeignete Maßnahmen getroffen werden, um den Betroffenen die in Art. 13 und 14 DS-GVO aufgeführten Angaben, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln. Dies kann schriftlich oder in einer anderen Form, z.B. elektronisch erfolgen.

Hinweis 18

Nach Art. 25 der DS-GVO müssen geeignete Mittel für die Verarbeitung festgelegt sowie technische und organisatorische Maßnahmen getroffen werden, die dazu ausgelegt sind, die Datenschutzvorgaben aus der Datenschutzverordnung wirksam umzusetzen und die Rechte der Betroffenen Personen zu schützen.