Verzeichnis der Verarbeitungstätigkeiten gem. Art. 30 Abs. 1 DSGVO für

komuna
EDV-Beratung für die Kommunalverwaltung

CIP - KD mit CIP - Archiv

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:	02.11.2023
Ausfüllende Person:	Jasmin Göring
Telefonnummer:	09548/982026-11

Bezeichnung der Verarbeitung (Hinweis Nr. 2):
Verarbeitung personenbezogener Daten und verfahrensbedingter Hinweise bei der Erledigung aller finanzwirtschaftlichen und kassenrechtlichen Angelegenheiten des Verantwortlichen inkl. Archivierung, elektronisches Anordnungswesen, Zahlungsabwicklung und Verbrauchsabrechnung

Übergeordneter Geschäftsprozess:
-
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:
CIP - KD mit CIP - Archiv - in der jeweils aktuellen Version **(Hinweis Nr. 5)**

1.2 Angaben zum Verantwortlichen:

Behörde/Einrichtung	Markt Wachenroth
Anschrift	Hauptstraße 23, 96193 Wachenroth
Verantwortliche Führungskraft:	1. Bürgermeister, Reiner Braun
Kontaktdaten:	09548/982026-10
Vertreter :	2. Bürgermeister, Felix Knorr
Kontaktdaten:	09548/982026-0
Ansprechpartner, sofern nicht verantwortliche Führungskraft:	Jürgen Reingruber
Kontaktdaten:	09548/982026-16

1.3 Angaben zum Datenschutzbeauftragten, sofern gemäß Art. 37 DSGVO benannt:

Name	Firma IfS, Herr Kiesl
Anschrift	An der Leite 16, 96193 Wachenroth
Kontaktdaten:	09548/982027-0

1.4 Angaben zum Auftragnehmer, sofern Auftragsverarbeitung gemäß Art. 28 DSGVO : **(Hinweis Nr. 6)**

Name	komuna GmbH EDV-Beratung
Anschrift	Wallerstraße 2; 84032 Altdorf
weitere? Name:	mps public solutions gmbh
Anschrift	Maria Trost 1; 56070 Koblenz

weitere? Name:	kiC Gesellschaft für Softwareentwicklung mbH
Anschrift	Am Hohen Kreuz 4 A, 96117 Memmelsdorf

(bei Datenmigration, Einrichtung, Dienstleistungen, anwendungsbezogener Fehlerbehebung, Support (auch im laufenden Betrieb evtl. mit Fernwartung), u.a.)

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

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

Erfüllung gesetzlicher Vorgaben und Verpflichtung im Rahmen der Verwaltungstätigkeit des Verantwortlichen bei der Erledigung aller finanzwirtschaftlichen und kassenrechtlichen (Haushalts-/ Kassen-/ Anordnungs-/ Steuer-/ Abgabenwesen) Angelegenheiten in der Behörde inkl. Archivierung, elektronisches Anordnungswesen, Zahlungsabwicklung und Verbrauchabrechnung

2.2 Rechtsgrundlage (zutreffende bitte ankreuzen und erläutern)

☒ Spezialgesetzliche Regelung außerhalb der DSG-VO
(Bitte benennen: Vorschrift, Paragraph, Absatz, Satz)
Grundgesetz für die Bundesrepublik Deutschland (GG) + Verfassung des Freistaates Bayern + Bürgerliches Gesetzbuch (BGB) für haushaltsrechtliche Grundsätze
Gemeindeordnung für den Freistaat Bayern (GO)
Landkreisordnung (LKrO)
Verwaltungsgemeinschaftsordnung (VGemO)
Abgabenordnung (AO)
Kommunalabgabengesetz (KAG)
Bayerische Haushaltsordnung (BayHO)
Zuwendungsvorschriften
Kommunalhaushaltsverordnung – Kameralistik (KommHV - Kameralistik)
Kommunalhaushaltsverordnung – Doppik (KommHV - Doppik)
zuzüglich der jeweiligen Ausführungsverordnungen und Verwaltungsvorschriften zur KommHV - Kameralistik und KommHV – Doppik
Kommunal Prüfungsverordnung (KommPrV)
Gemeindehaushaltsverordnung (GemHVO)
Gewerbesteuergesetz (GewStG)
Grundsteuergesetz (GrStG)
Grunderwerbsteuergesetz (GrEStG)
Körperschaftssteuergesetz (KStG)
Umsatzsteuergesetz (UStG)
Sozialgesetzbuch (SGB)
Insolvenzordnung (InsO)
eigene gemeindliche/ kommunale erlassene Satzungen (z.B. Gebührensatzung Verbrauch) und Dienstanweisungen (z.B. Scan-DA, DA für das Finanz- und Kassenwesen DA für Handvorschüsse)
Bayerisches Feuerwehrgesetz (BayFwG)
Finanzausgleichsgesetz (FAG) und FAGDV
Zivilprozessordnung (ZPO)
Verwaltungs- Zustellungs- und Vollstreckungsgesetz (VwZVG)
Bayerisches Kinderbildungs- und -betreuungsgesetz (BayKiBiG)
Bayerisches Schulfinanzierungsgesetz (BaySchFG)
Gesetz über die Kostenfreiheit des Schulweges (SchKfrG)

☐ weitere?
< 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)	
Siehe Anlage 1	Siehe Anlage 1	☐ Ja Welche:	☒ 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 (Archive) in derselben Verwaltungseinheit, der auch die Finanzabteilung angehört
Art der Daten	erforderliche und gesetzlich zugelassene Daten
Zweck der Daten-Mitteilung	zur Erfüllung der Aufgaben im jeweiligen Zuständigkeitsbereich (z.B. Gebührenkassen, Archivauskünfte)

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

Externe Stelle	Geldinstitute
Art der Daten	erforderliche und gesetzlich zugelassene Daten
Zweck der Daten-Mitteilung	zur Erfüllung der Aufgaben im jeweiligen Zuständigkeitsbereich (Zahlungsverkehrsabwicklung)

Externe Stelle	Finanzämter
Art der Daten	erforderliche und gesetzlich zugelassene Daten
Zweck der Daten-Mitteilung	zur Erfüllung der Aufgaben im jeweiligen Zuständigkeitsbereich (Steuerprüfungen)

Externe Stelle	Rechtsaufsichts-/ Prüfungsbehörde
Art der Daten	erforderliche und gesetzlich zugelassene Daten
Zweck der Daten-Mitteilung	zur Erfüllung der Aufgaben im jeweiligen Zuständigkeitsbereich (Genehmigungen, Rechnungsprüfungen)

Externe Stelle	Bayerischer Kommunaler Prüfungsverband
Art der Daten	erforderliche und gesetzlich zugelassene Daten
Zweck der Daten-Mitteilung	zur Erfüllung der Aufgaben im jeweiligen Zuständigkeitsbereich (Haushaltsrechnungs- und Datenprüfungen)

Externe Stelle	andere öffentliche Stellen (Regierungen)
Art der Daten	erforderliche und gesetzlich zugelassene Daten
Zweck der Daten-Mitteilung	zur Erfüllung der Aufgaben im jeweiligen Zuständigkeitsbereich (z.B. Zuwendungsanträge)

Externe Stelle	Mandatsträger (z.B. Steuerberater - nur bei expliziter Vollmacht des jeweiligen Betroffenen)
Art der Daten	erforderliche und gesetzlich zugelassene Daten
Zweck der Daten-Mitteilung	zur Erfüllung der Aufgaben im jeweiligen Zuständigkeitsbereich (Jahresabschlüsse der Mandanten)

Externe Stelle	Statistikbehörden
Art der Daten	erforderliche und gesetzlich zugelassene Daten
Zweck der Daten-Mitteilung	zur Erfüllung der Aufgaben im jeweiligen Zuständigkeitsbereich

Externe Stelle	Gerichtsvollzieher
Art der Daten	erforderliche und gesetzlich zugelassene Daten
Zweck der Daten-Mitteilung	zur Erfüllung der Aufgaben im jeweiligen Zuständigkeitsbereich (z.B. Forderungsbeitreibung)

Weitere externe Empfänger?

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:

☐ Nein

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

Zehn Jahre aufzubewahren sind Geschäftsbücher, Inventare, Eröffnungsbilanzen, Jahresabschlüsse, die zu ihrem Verständnis erforderlichen Arbeitsanweisungen und Organisationsunterlagen sowie die entsprechenden Buchungsbelege (kaufmännisch/ steuerrechtlich), nach dem Ende des jeweiligen Haushaltsjahres.
Geschäftsbriefe und sonstige Unterlagen, die für die Besteuerung von Bedeutung sind, sind für sechs Jahre aufzubewahren. Diese Frist gilt auch für Lohnkonten, sofern sie nicht Bestandteil der Buchführung sind (kaufmännisch/ steuerrechtlich).
Evtl. sind in den eigenen gemeindlichen/ kommunalen Satzungen entsprechende andere Vorgaben enthalten.
Den Zeitpunkt für die Vernichtung der papiergebundenen Belegdokumente legt die Kasse in Abstimmung mit dem örtlichen Rechnungsprüfungsorgan fest. Er sollte jedoch nicht vor dem Abschluss der Prüfung des Jahresabschlusses liegen. Soweit Bücher mit Hilfe automatisierter Verfahren geführt werden, können begründende Unterlagen dauerhaft auf geeigneten nicht veränderbaren elektronischen Speichermedien übernommen werden (WORM-Speicher).
Die Löschung erfolgt durch manuelle Betätigung entsprechender konfigurierbarer Löschungsfunktionalitäten im Modul und ist durch befugte Mitarbeiter in Eigenverantwortung umzusetzen.
Eine manuelle einzelfallbezogene Löschung einzelner Daten ist programmseitig jederzeit möglich und implementiert, sofern nicht andere Aufbewahrungsfristen hier wiederrum entgegen stehen (z.B. Fehleingaben welche nach erfolgtem Buchungslauf festgestellt werden, sind nicht löschbar - Haushaltsgrundsätze (Nachvollziehbarkeit))

6. Mittel der Verarbeitung

Welche Software oder Systeme werden für diese Verarbeitung eingesetzt?

Bezeichnung	Hersteller	Funktionsbeschreibung	Bereitstellung
CIP - KD	mps public solutions gmbh	Fachverfahren zur Erledigung des kommunalen Haushaltswesen	☐ Eigenentwickelte / Individual Software ☒ Standard- bzw. Kauf-Software ☐ Cloud-Services

Bezeichnung	Hersteller	Funktionsbeschreibung	Bereitstellung
CIP - Archiv	kiC Gesellschaft für Softwareentwicklung mbH	Verfahren zur Archivierung von verschiedensten Dokumenten (Belege, Tagesabschluss, Sollliste, Bescheide, usw.) des kommunalen Haushaltswesen	☐ Eigenentwickelte / Individual Software ☒ Standard- bzw. Kauf-Software ☐ Cloud-Services
komuna.NET	MR-Soft	Verfahren zur sicheren Übertragung personenbezogener Daten	☐ Eigenentwickelte / Individual Software ☒ Standard- bzw. Kauf-Software ☐ Cloud-Services
FAST SCC	FAST LTA AG	WORM-Speichermedium	☐ 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
< Text >	< Text >	< Text >	☐ Lesen ☐ Schreiben ☐ Löschen	< Text >
< 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: (ggf. als Anlage anfügen)
Berechtigungen sind nur im vorgegebenen Rahmen vergeben (Sachbearbeiter, Vertretung)

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:

Verfügbarkeit
Personenbezogene Daten stehen bei berechtigtem Bedarf zeitnah zur Verfügung um ordnungsgemäß und gesetzes- bzw. satzungskonform ausgewertet bzw. verarbeitet werden zu können:

Die Daten einer Person können in CIP - KD und CIP - Archiv schnell über Suchfunktionen (z.B. über Suche nach Name, Anschrift, Bankverbindung, usw.) aufgerufen werden und stehen dann für den Bearbeiter sofort zur Verfügung. Die Einarbeitung von Änderungen erfolgt unmittelbar.
Für Havariefälle hat die Behörde entsprechende Sicherheitssysteme einzusetzen (Parallelsysteme, Datensicherungsmanagement), die eine zeitnahe Weiterarbeit ermöglichen.

Integrität

Personenbezogene Daten bleiben während der Verarbeitung unversehrt, vollständig und aktuell, sofern diese nicht durch den jeweiligen verantwortlichen Sachbearbeiter bewusst korrigiert/ geändert werden.
Natürlich wird der Test der Software als ein integraler Bestandteil der Entwicklung gesehen.

Vertraulichkeit

Personenbezogene Daten sind nur befugten Personen zugänglich:
CIP – KD und CIP – Archiv sind generell 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, Datenbanken und Dateien sowie Passwortpflege und automatische Bildschirmdeaktivierung. Personenbezogene Daten, die an berechtigte Dritte elektronisch weitergegeben werden, sind in Absprache mit den Empfängern grundsätzlich zu verschlüsseln.

Weiterer Schutz der Rechte und Freiheiten der Betroffenen

Authentizität:

Innerhalb der Software werden alle Stammdatenänderungen und Buchungen hinsichtlich des durchführenden Mitarbeiters, des Zeitpunktes und des Inhaltes der Änderung protokolliert

Revisionsfähigkeit:

Durch Beauftragte kann jederzeit festgestellt werden, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat:
Alle Vorgänge, Änderungen usw., die von Programmnutzern einer Behörde an personenbezogenen Daten getätigt wurden, werden von CIP - KD bzw. CIP - Archiv intern mit Benutzernamen und Zeitstempel protokolliert und lassen sich später über die integrierte Auditfunktion jederzeit einsehen bzw. auswerten.

Transparenz:

Es ist sichergestellt, dass die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig und aktuell sind und derart dokumentiert werden, dass sie in angemessener Zeit nachvollziehbar sind:
Jeder Vorgang der sich auf die Verarbeitung personenbezogener Daten bezieht, wird von CIP - KD bzw. CIP - Archiv intern protokolliert und lässt sich schnell nachvollziehen
Betroffene, von denen personenbezogene Daten gespeichert sind, haben jederzeit die Möglichkeit in sämtliche über sie gespeicherte Daten Einsicht zu nehmen (Ausdrucke aus der Software).

9. Datenübertragbarkeit (Hinweis 16)

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

☒ Ja, Format: die Daten werden üblicherweise im .pdf-, xls-, txt-, dbf- oder csv-Format ausgegeben.

☐ Nein

10. Information der Betroffenen (Hinweis 17)

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

In CIP - KD und CIP - Archiv ist es möglich, dem Betroffenen vor Ort eine Auswertung (Ausdruck) zu übergeben, auf dem alle in der Software gespeicherten Stammdaten zu seiner Person ersichtlich sind. hieraus ist aber nicht ersichtlich in welchen weiteren Dokumenten/ Dateien/ Scans seine Daten noch erfasst sind (ggf. sind zusätzliche manuelle Suchläufe mit verschiedenen Kriterien nötig).
Diese Auswertungen sind von der Behörde jedoch noch mit den Informationen zu den individuellen Empfängern von Datenübermittlungen (intern, extern) zu ergänzen (mit Nennung des Verantwortlichen sowie des Datenschutzbeauftragten in der Behörde).

11. Datenschutz durch Technikgestaltung und Voreinstellungen (Hinweis 18)

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

☒ Ja
☐ Nein

Anmerkungen:
Hinsichtlich einer Benutzerkontrolle ist CIP - KD und CIP - Archiv 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 zugreifen.
Hinsichtlich der Zugriffskontrolle werden in CIP - KD und CIP - Archiv unterschiedliche Nutzer mit unterschiedlichen Berechtigungen angelegt, um eine individuelle und differenzierte Rechteverwaltung aufzubauen.
Bezüglich der Datenverarbeitungskontrolle sind sowohl CIP - KD als auch CIP - Archiv mit einer Vielzahl von Prüfalgorithmen ausgerüstet, die permanent die Integrität der Daten prüfen.
Die Verantwortlichkeits- und Dokumentationskontrolle wird in den Verfahren erreicht, in dem von den Nutzern (auch Administratoren) alle Vorgänge und Änderungen mit den jeweiligen Benutzernamen und einem Zeitstempel protokolliert werden. Diese Protokolldaten lassen sich jederzeit auswerten.

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

Die nachfolgenden Kategorien und Arten stehen nur auszugsweise für die typischerweise verarbeiten Daten:

Datenkategorien und Betroffene

- Personendaten
- Kommunikationsdaten
- Vertragsdaten
- Historiendaten
- Abrechnungs- und Zahlungsdaten
- Bankdaten
- Steuerdaten*
- Mahnungs-/ Vollstreckungsdaten*
- Buchhaltungsdaten
- Objektdaten
- Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
- sowie alle weiteren Kategorien aufgrund rechtlicher, gesetzlicher oder sonstiger Vorgaben vom Verantwortlichen in dessen Zuständigkeit und alleiniger Verfügungsgewalt in den jeweiligen Softwareprodukten erfassten und gespeicherten Daten

- Bürger/ Einwohner
- Steuerpflichtige
- Abgabepflichtige
- Bescheidempfänger
- Miteigentümer
- Beschäftigte/ Mitarbeiter
- Anwender/ User
- gesetzl. Vertreter
- Vormundschaften
- Lieferanten
- Zahlungsempfänger

* Werden die Module Steuern/ Abgaben und/ oder Mahnung/ Vollstreckung nicht eingesetzt, entfallen diese Kategorien

Datenarten:

- Name
- Vorname(n)
- Anrede
- Titel
- Adresse
- PLZ Ort
- Postfach Anschrift
- Kommunikationsdaten (Telefon, E-Mail, Telefax)
- Bankverbindungen (IBAN, BIC)
- Steuer- bzw. Objekt-Nummer + Objektbezeichnung
- Sonstige spezielle Daten für die jeweilige Gefällsart (z.B. Name des Kindes für KiGa-Beiträge)
- Verbrauchsabrechnungsdaten
- Grundstücksdaten + Flächenangaben
- Messbetrag bzw. Sollstellungsbetrag
- Aktenzeichen des Finanzamtes
- Daten zum gesetzlichen Vertreter
- Insolvenzangaben
- Fremdenverkehrsbeitrag
- Umsätze/ Gewinne lt. Abgabeerklärung
- Buchungstexte
- Anordnungstexte
- Verwendungszwecke
- Bediener
- Prüfvermerke (örtlich, überörtlich, inkl. Bemerkungen)
- sowie alle weiteren - in den eigenen Datenbankfeldern (z.B. Bemerkungen) - aufgrund rechtlicher, gesetzlicher oder sonstiger Vorgaben vom Verantwortlichen in dessen Zuständigkeit und alleinigen Verfügungsgewalt in den jeweiligen Softwareprodukten erfassten und gespeicherten Daten.

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 strukturierten, 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.