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

komuna
EDV-Beratung für die Kommunalverwaltung

komuna.RIS
Modul:
Sitzungsdienst mit Ratsinformationssystem und Ratsinfo-App

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:	09548/982026-16

Bezeichnung der Verarbeitung (Hinweis Nr. 2):
Verarbeitung personenbezogener Daten und verfahrensbedingter Hinweise im Rahmen der allgemeinen Verwaltungstätigkeit - hier bei der Abwicklung des Sitzungsdienstes (Vorlagen, Einladungen, Beschlüsse, Niederschriften, Bekanntmachungen), der Sitzungsgeldabrechnung sowie bei der Veröffentlichung von Sitzungsterminen und Sitzungsunterlagen, bzw. Darstellung der Gremiumsmitglieder/ Funktionsträger inkl. Zuständigkeiten und Zugehörigkeiten im Ratsinformationssystem (übers Internet) - zur Information der Bürger (öffentlicher Teil) und zur Sitzungsvorbereitung der Gremiumsmitglieder (öffentlicher + nichtöffentlicher Teil inkl. weiterer vertiefender Unterlagen);
Desweiteren besteht für berechtigte Gremiumsmitglieder eine Zugriffs- und Nutzungsmöglichkeit über die Ratsinfo-App (Erweiterung des Ratsinformationssystems für mobile Geräte)

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:
„komuna.RIS – Modul: Sitzungsdienst, Ratsinformationssystem und Ratsinfo-App“ der Firma kiC in der jeweils aktuellen Version **(Hinweis Nr. 5)**

1.2 Angaben zum Verantwortlichen:

Behörde/Einrichtung	Markt Wachenroth
Anschrift	Hauptstr. 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:	Jasmin Göring
Kontaktdaten:	09548/982026-11

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

Name	Ifs Sicherheitstechnik GmbH, 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:	kiC Gesellschaft für Softwareentwicklung mbH
Anschrift	Am Hohen Kreuz 4 A, 96117 Memmelsdorf

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

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

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

Sitzungsdienst:
Erfüllung gesetzlicher Vorgaben und Verpflichtungen im Rahmen der allgemeinen Verwaltungstätigkeit – hier bei der Abwicklung des Sitzungsdienstes (Vorlagen, Einladungen, Beschlüsse, Niederschriften, Bekanntmachungen) und der Sitzungsgeldabrechnung

Ratsinformationssystem und Ratsinfo-App: - sofern vorhanden -
Veröffentlichung von Sitzungsterminen und Sitzungsunterlagen bzw. Darstellung der Gremiumsmitglieder/ Funktionsträger inkl. Zuständigkeiten und Zugehörigkeiten im Ratsinformationssystem (übers Internet) - zur Information der Bürger (öffentlicher Teil) und zur Sitzungsvorbereitung der Gremiumsmitglieder (öffentlicher + nichtöffentlicher Teil inkl. weiterer vertiefender Unterlagen)

Ratsinfo-App: - sofern vorhanden -
Für berechtigte Gremiumsmitglieder besteht zusätzlich eine Zugriffs- und Nutzungsmöglichkeit über die Ratsinfo-App (Erweiterung des Ratsinformationssystems für mobile Geräte)

Hinweis:
Zwischen der Verwaltung und den Gremiumsmitgliedern sollte eine eigene Nutzungsvereinbarung (Umgang, Verhalten, Vertraulichkeit, usw.) bezüglich der zusätzlichen Nutzungsmöglichkeiten und bereitgestellten Information im Ratsinformationssystem und der Ratsinfo-App nach erfolgtem Login abgeschlossen sein.

2.2 Rechtsgrundlage (zutreffende bitte ankreuzen und erläutern)

☒ Spezialgesetzliche Regelung außerhalb der DSG-VO
(Bitte benennen: Vorschrift, Paragraph, Absatz, Satz)
Allgemeine Geschäftsordnung für Behörden des Freistaates Bayern (AGO)
(u.a. zur Schriftgutaufbewahrung §10 und §27 AGO)
Gemeindeordnung für den Freistaat Bayern (GO)
Bayerisches Archivgesetz (BayArchivG)
Bundesdatenschutzgesetz sowie jeweiliges Landesdatenschutzgesetz (BayDSG)
Die jeweilige eigene Geschäftsordnung des Verantwortlichen/ der Behörde/ des Gremiums
Alle sonstigen anwendbaren Rechtsgrundlagen und erlassenen Dienstanweisungen des Verantwortlichen aus denen sich weitere Informationen, Vorgaben und Vorschriften für die Verwendung und den Umgang mit einem Dokumentenmanagementsystem ergeben

☐ 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 ☐ Nein Welche: Je nach den verarbeiteten Dokumenten ist alles möglich und denkbar, auch Lichtbilder und Parteizugehörigkeiten

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,
Art der Daten	erforderliche und gesetzlich zugelassene Daten
Zweck der Daten-Mitteilung	zur Erfüllung der Aufgaben im jeweiligen Zuständigkeitsbereich (z.B. Kasse zur Erstattung von Sitzungsgeldern oder Bauhof zur Erledigung von zugewiesenen Aufgaben bzw. zur Beseitigung von Mängeln)

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	Finanzamt
Art der Daten	erforderliche und gesetzlich zugelassene Daten
Zweck der Daten-Mitteilung	zur Erfüllung der Aufgaben im jeweiligen Zuständigkeitsbereich (z.B. Bescheinigung der bezogenen Sitzungsgelder auf Anfrage))

Externe Stelle	Rechtsaufsichts-/ Prüfungsbehörde
Art der Daten	erforderliche und gesetzlich zugelassene Daten
Zweck der Daten-Mitteilung	zur Erfüllung der Aufgaben im jeweiligen Zuständigkeitsbereich (z.B. 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 (IT- 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
Art der Daten	erforderliche und gesetzlich zugelassene Daten

Zweck der Daten-Mitteilung	zur Erfüllung der Aufgaben im jeweiligen Zuständigkeitsbereich (z.B. Sitzungsunterlagen/ Niederschriften)
Externe Stelle	sonstige Behörden bzw. öffentliche Dienststellen bzw. private Dritte
Art der Daten	erforderliche und gesetzlich zugelassene Daten
Zweck der Daten-Mitteilung	zur Erfüllung rechtlicher/ gesetzlicher Verpflichtungen und Durchführung/ Erledigung der Aufgaben im jeweiligen Zuständigkeitsbereich. (z.B. Mitteilung/ Abgleich aller Vereinsvorstände mit dem Landratsamt für ein Anschreiben durch dieses)
Externe Stelle	Polizei- und Ordnungsbehörden
Art der Daten	erforderliche und gesetzlich zugelassene Daten
Zweck der Daten-Mitteilung	zur Erfüllung der Aufgaben im jeweiligen Zuständigkeitsbereich
Externe Stelle	komuna GmbH
Art der Daten	erforderliche und gesetzlich zugelassene Daten
Zweck der Daten-Mitteilung	zur Erfüllung der Aufgaben im jeweiligen Zuständigkeitsbereich (hier Hosting des Ratsinformationssystems)

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:

Es gelten u.a. Art. 12 BayDSG sowie die jeweiligen Aufbewahrungs- und Löschfristen aus den sonstigen betroffenen Rechtsgrundlagen, sofern nicht eine andere zu beachtende Rechtsvorschrift (z.B. Archivgesetz oder Dienstanweisungen) eine Löschung untersagen (z.B. Niederschriften und Beschlussvorlagen werden nicht gelöscht, da diese für künftige Planungen, Auswertungen und Recherchen zur Verfügung stehen müssen).

☐ Nein

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

Eine manuelle einzelfallbezogene Löschung einzelner Dokumente/ Daten ist programmseitig jederzeit möglich und implementiert.
Die Löschung erfolgt durch manuelle Betätigung entsprechender konfigurierbarer Löschungsfunktionalitäten im Modul und ist durch befugte Mitarbeiter in Eigenverantwortung umzusetzen.

6. Mittel der Verarbeitung

Welche Software oder Systeme werden für diese Verarbeitung eingesetzt?

Bezeichnung	Hersteller	Funktionsbeschreibung	Bereitstellung
komuna.RIS Modul: Sitzungsdienst mit Ratsinformationssystem und Ratsinfo-App	kiC Gesellschaft für Softwareentwicklung mbH	Siehe Bezeichnung des Verfahrens und Zweck	☐ 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)
< Text >

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 komuna.RIS Modul Sitzungsdienst schnell über Suchfunktionen (z.B. über Suche nach Vor- oder Nachnamen) 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:
komuna.RIS Modul Sitzungsdienst ist generell passwortgeschützt. Jeder berechtigte Mitarbeiter einer Behörde (namentlich benannt) muss sich mit einem eindeutigen Benutzernamen und Passwort 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. 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 wird die letzte Änderung hinsichtlich des durchführenden Mitarbeiters und des Zeitpunktes protokolliert, jedoch nicht was geändert wurde.

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:

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 können üblicherweise im pdf-, csv-, docx-oder vcf-Format ausgegeben werden.

☐ 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 komuna.RIS Modul Sitzungsdienst ist es möglich, dem Betroffenen vor Ort eine Auswertung (Ausdruck) zu übergeben, auf dem die in der Software gespeicherten Stammdaten ersichtlich sind, hieraus ist aber nicht ersichtlich in welchen weiteren Dokumenten/ Dateien seine Daten noch erfasst sind (ggf. sind weitere 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 Datenschutz durch Technikgestaltung und der datenschutzfreundlichen Voreinstellungen eingehalten?

☒ Ja

☐ Nein

Anmerkungen:

Hinsichtlich einer Benutzerkontrolle ist komuna.RIS Modul Sitzungsdienst 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 unterschiedliche Nutzer oder Nutzergruppen mit unterschiedlichen Berechtigungen angelegt, um eine individuelle und differenzierte Rechteverwaltung aufzubauen.

Die Verantwortlichkeits- und Dokumentationskontrolle wird in dem Verfahren erreicht, in dem von den Nutzern (auch Administratoren) die letzte Änderung mit den jeweiligen Benutzernamen und einem Zeitstempel protokolliert wird. Diese Protokolldaten lassen sich auswerten.

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

Da in einem Sitzungsdienstsystem bekanntlich die unterschiedlichsten Dokumente und Dateien verarbeitet werden, und jeder Nutzungs- und Zugriffsberechtigte in seiner Entscheidung frei ist, welche Inhalte der Bearbeiter in den Dokumenten/ Dateien erfasst und speichert, ist eine umfassende und lückenlose Auflistung aller möglichen betroffenen Kategorien und Arten von personenbezogenen Daten nicht möglich.

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

Datenkategorien und Betroffene

- Personendaten
- Kommunikationsdaten
- Vertragsdaten
- Historiendaten
- Planungs- und Steuerungsdaten
- Abrechnungs- und Zahlungsdaten
- 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
- Unternehmen/ Gewerbetreibende
- Ansprechpartner
- Vereinsvorstände
- Steuerpflichtige
- Abgabepflichtige
- Bescheidempfänger
- Miteigentümer
- Beschäftigte/ Mitarbeiter/ Ehemalige
- Anwender/ User
- gesetzl. Vertreter
- Lieferanten
- Parteien/ Verbände/ Gruppierungen
- Mandatsträger/ Gremien/ Ausschüsse
- Sitzungsteilnehmer (z.B. Sachverständige, Antragsteller)
- sowie alle weiteren möglichen Betroffenen aufgrund rechtlicher, gesetzlicher oder sonstiger Vorgaben vom Verantwortlichen in dessen Zuständigkeit und alleiniger Verfügungsgewalt in den jeweiligen Softwareprodukten erfassten und gespeicherten Daten

Datenarten:

<u>Persönliche Stammdaten sind u.a.</u>

- Anrede
- Anredetext
- Firmenname*
- Titel*
- Akademischer Grad*
- Name
- Vorname*
- Straße, Hausnummer und Ortsteil*
- Postleitzahl und Ort*
- Telefon, Fax und Mobiltelefon (Privat)*
- Internet- und Email-Adresse (Privat)*
- Telefon, Fax und Mobiltelefon (Arbeitgeber)*
- Internet- und Email-Adresse (Arbeitgeber)*
- Bankverbindung (IBAN, BIC, Kontoinhaber)*
- Zusatzfeld - frei eingebbar z.B. für Ehrenämter*
- Berufsbezeichnung (Funktion) - Kurzbezeichnung (Funktion)*
- Weitere Anschrift, z.B. Arbeitgeber mit Adresse und Telefonverbindung*
- Firmenzugehörigkeit*
- Zuordnung zu Kategorie - z.B. Vereinsvorstand oder Gemeinderatsmitglied*
- Selbständigkeit (wird zur Sitzungsgeldabrechnung benötigt)*
- Geburtsdatum*

- Politische Tätigkeit*
- Ehrenamtliche Tätigkeit und Mitgliedschaft in Vereinen*
- Selbstdarstellung*
- Porträt*

Zusätzlich nur für Mitarbeiter
- Zimmernummer, Mitarbeiterkürzel, Durchwahl, Email etc. in der Verwaltung

Gremiendaten:
- Bezeichnung des Gremiums
- Funktion, z.B. 1. Bürgermeister, Vorsitzender, etc.
- Zeitraum, Zugehörigkeit zu Gremien und Ausschüssen
- Vertretertätigkeit*
- Stimmberechtigung*
- Anwesenheit bei Sitzungen (als Mitglied, Vertreter oder nur zur Kenntnisnahme)*
- Zugehörigkeit zu Fraktionen*

Sitzungsgelddaten:
- Sitzungsgeldart (Pauschale, Betrag pro Sitzung, Zuschlag bei Selbständigkeit, etc.
- Sitzungsgeldhöhe

Ratsinformationssystem + Ratsinfo-App:
- Benutzerdaten (Login für geschützten Bereich)
- Erlaubter Bereich, z.B. Beschlussvorlagen öffentlich und nichtöffentlich, je nach Konfiguration der Verwaltung

- sowie alle weiteren Arten aufgrund rechtlicher, gesetzlicher oder sonstiger Vorgaben vom Verantwortlichen in dessen Zuständigkeit und alleinigen Verfügungsgewalt in den jeweiligen Softwareprodukten erfassten und gespeicherten Daten.

* Ggfs. kann es sich um keine Pflichtangaben sondern um rein freiwillig/ optional auszufüllende Felder handeln (je nach Systemnutzung).

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.