

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: 04.01.2019
Ausfüllende Person: Jennifer Naue
Telefonnummer: 05335/801-36

- **Bezeichnung der Verarbeitung (Hinweis Nr. 2):** Verarbeitung personenbezogener Daten zur Regelung und Vereinfachung des Zahlungsverkehrs der Behörden aufgrund der relevanten kassenrechtlichen Bestimmungen.

Übergeordneter Geschäftsprozess: Autarke Verwendung oder Verwendung im Zusammenhang mit der Führung eines Melderegisters, Passregisters und Ausweisregisters oder anderer fachspezifischer Register

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: Modul „Gebührenkasse“ in der jeweils aktuellen Version (Hinweis Nr. 5)
- 1.2 Fachbereich: FB III – Bürgerservice und Ordnung
Verantwortliche Führungskraft: Herr Hendrik Brase
ggf. Stellen-Kennzeichen: Fachbereichsleiter
- 1.3 Ansprechpartner, sofern nicht verantwortliche Führungskraft: Frau Jennifer Naue
Telefon-Nummer: 05335/801-36
- 1.4 Name u. Anschrift des Auftragnehmers, wenn Auftragsverarbeitung nach Art. 28 DSGVO (Hinweis Nr. 6): HSH Soft- und Hardware Vertriebs GmbH, Rudolf-Diesel-Str. 2 in 16356 Ahrensfelde bei Datenmigration, Fehlerbehebung (auch im laufenden Betrieb mittels Fernwartung [Teamviewer],

Vertrags-Nummer: 2014-MESO_NSA/Schladen-Werla Vertrag zur Auftragsverarbeitung vom 28.06./05.07.2018.

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

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

Führung des Melderegisters gemäß §§ 2 bis 4 Bundesmeldegesetz (BMG)

Führung des Passregisters gemäß §§ 19, 21 und 22 Passgesetz (PassG)

Führung des Ausweisregisters gemäß §§ 7, 8 und 23 Gesetz über Personalausweise und den elektronischen Identitätsnachweis (PAuswG).

2.2 Rechtsgrundlage (zutreffende bitte ankreuzen und erläutern)

- Spezialgesetzliche Regelung außerhalb der DSGVO
§ 42 Verordnung über die Ausstellung und Ausführung des Haushaltsplans sowie die Abwicklung der Kassengeschäfte der Kommunen (Kommunalhaushalts- und –kassenverordnung – KomHKVO –)
- Einwilligung des Betroffenen (Art. 6 Abs. 1 a) DSGVO: 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) DSGVO.
< Text >
- Interessenabwägung (Art. 6 Abs. 1 f) DSGVO:
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)	
Personen, die Verwaltungshandlungen zu zahlen haben	Personendaten und Bankverbindungsdaten der zahlungspflichtigen Personen: Name Vorname (gebräuchlicher Vorname) gegenwärtige Anschrift Kontodaten (im unbaren Zahlungsverkehr außer bei Kostenbescheiden) Kartennummer (bei EC-Karten).	<input type="checkbox"/> Ja	<input checked="" type="checkbox"/> Nein

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

4.1 Interne Empfänger innerhalb der verantwortlichen Stelle

Interne Stelle (Org-Einheit)	Kämmereien und Stellen des Haushaltskostenrechnungswesens in der selben Verwaltungseinheit, der auch die Meldebehörde angehört
Art der Daten	erforderliche und gesetzlich zugelassene Daten aus dem Melderegister
Zweck der Daten-Mitteilung	zur Erfüllung der in § 37 BMG genannten Aufgaben

4.2 Externe Empfänger und Dritte (jeder andere Empfänger, auch Konzern-unternehmen)

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

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 Lösungsfristen?

Ja, falls ausgewählt bitte benennen: Die Lösungsfristen nach den Bestimmungen des Haushalts- und Kassenwesens sind zu berücksichtigen und einzuhalten. Eine programmseitige Einhaltung dieser Grundsätze ist realisiert.

Nein

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

Die Löschung (und ggfs. Archivierung) erfolgt sowohl automatisiert durch die Implementierung einer entsprechenden Aufgaben zum Löschen und Bereinigen von Registerdaten als auch durch manuelle Betätigung entsprechender Lösungsfunctionalitäten in den Registern.

Eine manuelle einzelfallbezogene Löschung einzelner Daten ist programmseitig jederzeit möglich und implementiert.

6. Mittel der Verarbeitung

Welche Software oder Systeme werden für diese Verarbeitung eingesetzt?

Bezeichnung	Hersteller	Funktionsbeschreibung	Bereitstellung
Gebührenkasse	HSH Soft- und Hardware Vertriebs GmbH	Fachverfahren zur Regelung und Vereinfachung des Zahlungsverkehrs	<input type="checkbox"/> Eigenentwickelte / Individual Software <input checked="" type="checkbox"/> Standard- bzw. Kauf-Software <input type="checkbox"/> 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
Mitarbeiter Bürgerservicebüro	Sachbearbeitung	Personendatenbank und Bankverbindungsdaten	<input checked="" type="checkbox"/> Lesen <input checked="" type="checkbox"/> Schreiben <input type="checkbox"/> Löschen	Sachbearbeitung
Mitarbeiter IT	Administratoren	Personendaten und Bankverbindungen	<input checked="" type="checkbox"/> Lesen <input checked="" type="checkbox"/> Schreiben <input type="checkbox"/> Löschen	Administration
< Text >	< Text >	< Text >	<input type="checkbox"/> Lesen <input type="checkbox"/> Schreiben <input type="checkbox"/> Löschen	< Text >

Bitte erläutern Sie kurz den Prozess zur Erlangung und Verwaltung der Berechtigungen oder benennen Sie das detaillierte betriebliche Berechtigungskonzept:

Berechtigungsvergabe durch die IT nach Bestätigung der dienstl. Erforderlichkeit durch den Fachbereichsleiter.

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 gesetzeskonform ausgewertet bzw. verarbeitet werden zu können:

Die Daten einer Person können in der Gebühreneinzelkasse schnell über Suchfunktionen (z.B. über Suche Namen, Daten oder Vorgängen) 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
Vertraulichkeit	<p>Personenbezogene Daten sind nur befugten Personen zugänglich (Benutzerverwaltung): Die Gebührenkasse ist generell passwortgeschützt. Jeder berechnigte Mitarbeiter einer Behörde (namentlich benannt) muss sich mit einem eindeutigen Benutzernamen und Passwort exklusiv anmelden. Eine parallele Nutzung des Programms mit gleicher Anmeldung ist ausgeschlossen. 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.</p>
Weiterer Schutz der Rechte und Freiheiten der Betroffenen	<p>Maßnahmen zur Gewährleistung der Revisionsfähigkeit: Durch Beauftragte kann jederzeit festgestellt werden, wer wann welche personenbezogenen Daten in Buchungsfällen in welcher Weise verarbeitet hat: Alle Vorgänge, Änderungen usw., die von Programmnutzern einer Behörde an personenbezogene Daten getätigt wurden, werden von der Gebührenkasse intern mit Benutzernamen und Zeitstempel protokolliert und lassen sich später jederzeit einsehen bzw. auswerten.</p> <p>Maßnahmen zur Gewährleistung der 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 der Gebührenkasse intern protokolliert und lässt sich schnell nachvollziehen. Betroffene, von denen personenbezogene Daten gespeichert sind, haben jederzeit die Möglichkeit in sämtliche über sie gespeicherten Daten Einsicht zu nehmen.</p>

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 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?

Im Programm sind entsprechende Informationsdokumentationen hinterlegt, die den Betroffenen zum einen Auskunft zu seinen gespeicherten Daten, zur Herkunft der in den Registern gespeicherten Daten sowie zu den Empfängern seiner personenbezogenen Daten geben.

Diese Informationen können dem Betroffenen vor Ort übergeben oder auch elektronisch zur Verfügung gestellt werden.

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 Gebührenkasse 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 in der Gebührenkasse unterschiedliche Nutzer oder Nutzergruppen mit unterschiedlichen Berechtigungen angelegt, um eine individuelle und differenzierte Rechteverwaltung aufzubauen.

Bezüglich der Datenverarbeitungskontrolle ist die Gebührenkasse mit einer Vielzahl von Prüfalgorithmen ausgerüstet, die permanent die Integrität der Daten prüfen.

Die Verantwortlichkeits- und Dokumentationskontrolle wird in der Fachanwendung Gebührenkasse 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.

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.