



Internetwahlschein OLIWA – Online-Wahlscheinvorgänge

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 beim Online-Beantragungsprozess im Wahlscheinverfahren und zur Wahlraumsuche über das Internet

Übergeordneter Geschäftsprozess: eGovernment

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:

Internetwahlschein (OLIWA – Online-Wahlscheinvorgänge) 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:	Jasmin Göring
Kontaktdaten:	09548/982026-11

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

Name	IfS Sicherheitstechnik, Herr Kiesel
Anschrift	An der Leite 16, 96193 Wachenroth
Kontaktdaten:	09548/982026-0

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:	HSH Soft- und Hardware Vertriebs GmbH
Anschrift	Rudolf-Diesel-Str. 2; 16356 Ahrensfelde
(bei Hosting, 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):

Online-Vorgang für den Beantragungsprozess im Wahlscheinverfahren und zur Wahlraumsuche über das Internet entsprechend Bundesmeldegesetz, Bundes- bzw. Landeswahlordnungen (beispielsweise §§ 27 ff. BWO)

2.2 Rechtsgrundlage (zutreffende bitte ankreuzen und erläutern)

- Spezialgesetzliche Regelung außerhalb der DSGVO
 (Bitte benennen: Vorschrift, Paragraph, Absatz, Satz)
- EGovernment-Gesetz
 - Bundesmeldegesetz und Ausführungsgesetze der Länder sowie entsprechende Verwaltungsvorschriften
 - Wahlgesetze der Europäischen Union, des Bundes und der Länder und entsprechende Verordnungen

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

Die Einwilligung wird vom Antragsteller ausdrücklich in einem eigenen Vorgangsschritt abgefragt und erhoben. Sie bedarf ausdrücklich in einem eigenen Schritt der aktiven Mitwirkung des Antragstellers (durch ankreuzen, programmseitig nicht vorgelegt).

Der jeweilige Text lautet für

OLIWA - Online-Wahlscheinvorgänge:

- „Die Datenschutzhinweise und Pflichtangaben habe ich zur Kenntnis genommen. Ich willige in die Verarbeitung meiner personenbezogenen Daten, die zum Zwecke der Bearbeitung meines Wahlscheinantrages über die gesetzlichen Pflichtangaben hinaus erhoben werden, freiwillig ein.“

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 wahlberechtigten Personen zu der jeweiligen Wahl	Familienname Vornamen und/ oder gebräuchlicher Vorname Tag der Geburt Anschrift Ggfs. abweichende Versandanschrift (Zustellungsanschrift) Wahlbezirk Optional: Nummer im Wählerverzeichnis Optional: E-Mail-Adresse, Telefonnummer, FAX IP-Adresse des Antragstellers Tag (Datum) und Uhrzeit der Antragstellung	<input type="checkbox"/> Ja Welche:	<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)	Meldebehörde
Art der Daten	erforderliche und gesetzlich zugelassene Daten aus den Onlinevorgang
Zweck der Daten-Mitteilung	zur Erfüllung der melderechtlich vorgegebenen Aufgaben
Interne Stelle (Org.-Einheit)	Wahlamt (soweit nicht Meldebehörde)
Art der Daten	erforderliche und gesetzlich zugelassene Daten aus den Onlinevorgang
Zweck der Daten-Mitteilung	zur Erfüllung der in den jeweilig anzuwendenden Wahlnormen genannten Aufgaben
Interne Stelle (Org.-Einheit)	Behörden und andere öffentliche Stellen in derselben Verwaltungseinheit
Art der Daten	erforderliche und gesetzlich zugelassene Daten aus dem Onlinevorgang
Zweck der Daten-Mitteilung	zur Erfüllung der Aufgaben im jeweiligen Zuständigkeitsbereich

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 und – vorgaben können systemseitig konfiguriert werden. Für die Daten des Melderegister gelten die Bestimmungen der §§ 13 bis 15 BMG

Nein

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

Die Löschung erfolgt sowohl automatisiert durch konfigurierte Aufgaben zum Löschen und Bereinigen von Registerdaten als auch durch manuelle Betätigung entsprechender Lösungsfunctionalitäten in den Registern.

6. Mittel der Verarbeitung

Welche Software oder Systeme werden für diese Verarbeitung eingesetzt?

Bezeichnung	Hersteller	Funktionsbeschreibung	Bereitstellung
OLIWA	HSH Soft- und Hardware Vertriebs GmbH	Fachverfahren zur Online-Beantragung von Wahlscheinen	<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
Wahlamt	< Text >	< Text >	<input checked="" type="checkbox"/> Lesen <input checked="" type="checkbox"/> Schreiben <input checked="" type="checkbox"/> Löschen	Bearbeitung

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

Berechtigungen werden nur im gesetzlich vorgeschriebenen Rahmen vergeben.

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. verarbeitet werden zu können:

In OLIWA erfasste Personendaten werden nach einem von der Wahlbehörde festgelegten Zeitplan in das Wahlverfahren übernommen und stehen dann für den Bearbeiter sofort zur Verfügung.

Die landesspezifischen Lösch- und Archivierungsvorgaben sind fester Bestandteil der Software und sind durch befugte Mitarbeiter in Eigenverantwortung umzusetzen. 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:

Darüber hinaus können mittels integrierter Prüfmodule sachbezogene Datenbankläufe zyklisch aktiviert werden, um eventuelle Daten-Inkonsistenzen aufzuspüren. Natürlich wird der Test der Software als ein integraler Bestandteil der Entwicklung gesehen

Vertraulichkeit

Personenbezogene Daten sind nur befugten Personen zugänglich:

Die Fachanwendungen sind generell passwortgeschützt. Jeder berechnigte 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 Maß-

nahmen zu ergreifen wie z.B. Zugriffsrechte auf Rechner, Verzeichnisse und Dateien sowie Passwortpflege und automatische Bildschirmdeaktivierung. Personenbezogene Daten, die an berechnigte Dritte elektronisch weitergegeben werden, sind in Absprache mit den Empfängern grundsätzlich zu verschlüsseln.

Weiterer Schutz der Rechte und Freiheiten der Betroffenen

Authentizität:

Personenbezogene Daten können jederzeit ihrem Ursprung zugeordnet werden:

Innerhalb der Software werden alle Änderungen hinsichtlich des durchführenden Mitarbeiters, des Zeitpunktes und des Inhaltes der Änderung protokolliert. Bei Bedarf ist es möglich zusätzliche Verweise auf den Ursprung bzw. die Herkunft der Daten zu speichern.

Revisionsfähigkeit:

Durch Beauftragte kann jederzeit festgestellt werden, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat:

Alle Verarbeitungen, die von Programmnutzern einer Behörde an personenbezogenen Daten getätigt wurden, werden intern mit Benutzernamen und Zeitstempel protokolliert und lassen sich später über die integrierte Controllingfunktion 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 intern protokolliert und lässt sich schnell nachvollziehen. Betroffene, von denen personenbezogene Daten gespeichert sind, haben jederzeit die Möglichkeit über sämtliche über sie erteilten Auskünfte Einsicht zu nehmen.

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-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 (Antragsdaten) 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 zur (gesicherten) Kommunikation:

Die Eingabe der Daten durch den Antragsteller erfolgt über gesicherte Kommunikationswege (HTTPS-Verschlüsselung). Die Abholung der Daten erfolgt ebenfalls über gesicherte Kommunikationswege (HTTPS). Die übertragenen Daten sind zusätzlich verschlüsselt. Die Abholung der Daten ist nur mit Benutzernamen und Passwort möglich. Mehrfache Versuche, die Daten mit einem falschen Passwort abzuholen, führen zur Sperrung des Nutzers.

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.