Zur Befüllung durch den externen Dienstleister:

(für Anwendungen, die über die FI bezogen werden: siehe Ausführung im UBK-DSGVO, Kap. 13.6. „Prüfung zur Einhaltung von Data Protection by Design und by Default - Art. 25 DSGVO“)

Prüfung zur Einhaltung von Data Protection by Design und by Default || Art. 25 DSGVO

Vertragspartner

Hersteller: Ogulo GmbH

Verwender:
(ggf. identisch mit dem Vertragspartner):

Zu prüfendes System:

Systembezeichnung/-name: Ogulo

Version: 2.13.8.355

vom: 14.04.2026

Zu prüfende Anwendung:

Anwendungsname:

Version:

vom:

Ablageort der Dokumentation: ☐ Kopie im Kontrollordner (siehe unten) ☐ SAM-Library ☐ Sonstiger Ablageort

Kontrolle

am:

durch NAME
Kontaktdaten d. Ansprechpartners beim Dienstleister:

Versand an Vertragspartner am durch

Voraussetzungen

- Bei Einsatz eines neuen Systems oder Prozesses ist zu prüfen, ob personenbezogene Daten i.S.d. Art. 4 Nr. 1 DSGVO verarbeitet werden sollen.
- Wenn personenbezogene Daten verarbeitet werden sollen, ist schon zu Beginn eines Einführungsverfahrens festzulegen, wie die Prinzipien von Data Protection by Design und Data Protection by Default eingehalten werden. Ferner sind die technischen und organisatorischen Maßnahmen darauf zu überprüfen bzw. darauf abzustellen.
- Um der Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO Folge zu leisten, sind die Systeme/Prozesse vor Inbetriebnahme diesbezüglich zu prüfen und das Ergebnis zu dokumentieren. Maßnahmen zur Sicherstellung des Gewährleistungsziels der Verfügbarkeit aus Sicht des Betroffenen werden in diesem Dokument nicht erfragt, da hier die Ziele des Unternehmens und des Betroffenen deckungsgleich sind. Das gleiche gilt für das Gewährleistungsziel der Belastbarkeit. In den nachfolgenden Ausführungen werden als „Stand der Technik“ marktgängige, etablierte Lösungen angesehen, die einen hohen Sicherheitsstandard aufweisen. Dazu zählen

unter anderem anerkannte Unternehmen bzw. Softwarelösungen, Spezialisten auf dem Gebiet auf datenschutzkonforme Umsetzungen und entsprechend zertifizierter Anbieter (z.B. durch BSI- oder ISO-Normen in Bezug auf Informationssicherheit). Es sollte unter Abwägung von Implementierungskosten und Risiken die beste verfügbare Technologie gewählt werden. Die Abwägung von Implementierungskosten und Risiken ist bereits bei der Beschaffung zu berücksichtigen und zu dokumentieren.

Frage	Erläuterung	Bitte treffen Sie eine Auswahl: Ja oder Nicht anwendbar, weil….. Bitte begründen Sie die jeweilige konkrete Maßnahme. Bei Verweisen auf Dokumentationen fügen Sie diese bitte bei, um die Aussage nachhaltig belastbar zu machen und der Rechenschaftsplicht nachzukommen.
I. Data Protection by Design		
I.1 Können einzelne Datensätze mit personenbezogenen Daten individuell gelöscht werden?	Es muss gewährleistet sein, dass Datensätze individuell löschbar sind. So können Betroffenenbegehren (insb. Art. 17 DSGVO) angemessen umgesetzt werden. Idealerweise sind Datensätze nicht nur vollständig, sondern auch partiell löschbar.	☒ Ja, die Anforderung ist umgesetzt durch folgende Maßnahme(n): Die Anforderung ist umgesetzt durch die individuelle Löschbarkeit einzelner Datensätze.
I.2 Ist die Sperrung einzelner Datensätze möglich?	Um das Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO) zu wahren, müssen Datensätze für die weitere Verarbeitung gesperrt werden können. Dabei ist zu beachten, dass die Sperrung reversibel sein muss, damit Rechte angemessen gewahrt werden können.	☒ Ja, die Anforderung ist umgesetzt durch folgende Maßnahme(n) Die Anforderung ist umgesetzt durch die Möglichkeit, einzelne Datensätze reversible für die weitere Verarbeitung zu sperren.
I.3 Ist die Zahl der Eingabefelder auf das Wesentliche begrenzt?	Gemäß dem Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO) müssen personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Daraus folgt, dass in einem System nur die Eingabefelder vorhanden sein sollten, deren Daten für die konkrete	☒ Ja, die Anforderung ist umgesetzt durch folgende Maßnahme(n) Die Anforderung ist umgesetzt durch die Beschränkung der Eingabefelder und Freitextfelder auf das unbedingt notwendige Maß.

Frage	Erläuterung	Bitte treffen Sie eine Auswahl: Ja oder Nicht anwendbar, weil….. Bitte begründen Sie die jeweilige konkrete Maßnahme. Bei Verweisen auf Dokumentationen fügen Sie diese bitte bei, um die Aussage nachhaltig belastbar zu machen und der Rechenschaftsplicht nachzukommen.
	Verarbeitung benötigt werden. Auf diese Weise soll eine Vorratsdatenspeicherung verhindert werden. Zudem sollte die Anzahl an Freitextfeldern auf das Notwendige minimiert werden. In Freitextfeldern werden des Öfteren persönliche Anmerkungen der Sachbearbeiter notiert, deren Inhalte im Falle der Bereitstellung einer Kopie im Rahmen der Betroffenenauskunft nach Art. 15 DSGVO auch negative Auswirkungen auf die Geschäftsbeziehung nach sich ziehen können.	
I.4 Sind Einwilligungen des Betroffenen dokumentierbar?	Falls personenbezogenen Daten über den ursprünglichen Zweck hinaus oder für Direktwerbung verwendet werden sollen, ist eine Einwilligung des Betroffenen einzuholen. Diese Einwilligung ist zu dokumentieren.	☒ Nicht anwendbar, weil Eine Dokumentation ist nicht erforderlich, da im System keine Einwilligungen für Werbung benötigt werden und die personenbezogenen Daten ausschließlich zweckgebunden verarbeitet werden.
I.5 Ist sichergestellt, dass bei fehlender bzw. widerrufener Einwilligung eine über den ursprünglichen Zweck hinausgehende Datenverarbeitung bzw.	Sofern die Einwilligung des Betroffenen widerrufen wird (bzw. gar nicht erst bestand), dürfen Datenverarbeitungen, die über den ursprünglichen Zweck der Datenerhebung hinausgehen, nicht (weiter) durchgeführt werden. Dies gilt insbesondere für die direkte Bewerbung des Kunden via Telefon oder	☒ Ja, die Anforderung ist umgesetzt durch folgende Maßnahme(n) Die Anforderung ist umgesetzt, da im System keine Verarbeitung über den ursprünglichen Zweck hinaus erfolgt und Direktwerbung ausgeschlossen ist.

Frage	Erläuterung	Bitte treffen Sie eine Auswahl: Ja oder Nicht anwendbar, weil….. Bitte begründen Sie die jeweilige konkrete Maßnahme. Bei Verweisen auf Dokumentationen fügen Sie diese bitte bei, um die Aussage nachhaltig belastbar zu machen und der Rechenschaftsplicht nachzukommen.
Direktwerbung nicht länger möglich sind?	elektronischer Medien.	
I.6 Ist sichergestellt, dass nur der für die Erfüllung der Datenverarbeitung notwendige Personenkreis Zugriff auf die personenbezogenen Daten erhält?	Im Rahmen der technischen und organisatorischen Maßnahmen muss durch ein entsprechendes Rechte- und Rollenkonzept sichergestellt sein, dass nur die Mitarbeiter, die tatsächlich personenbezogene Daten verarbeiten müssen, Zugriff auf diese Daten erhalten. Zu umfangreiche Zugriffsrechte erhöhen das Risiko, dass Daten ohne Rechtsgrundlage oder für nicht legitime Zwecke verarbeitet werden könnten.	☒ Ja, die Anforderung ist umgesetzt durch folgende Maßnahme(n) Die Anforderung ist umgesetzt, da ausschließlich Makler derselben Firma Zugriff auf die jeweiligen Interessendaten haben.
I.7 Sind Möglichkeiten zur Erfüllung von Betroffenenanfragen gegeben?	Neben den Rechten zur Löschung bzw. Einschränkung der Bearbeitung (s.o.) sind insbesondere folgende Rechte von größerer Relevanz: • Recht aus Auskunft, Art. 15 DSGVO • Recht auf Berichtigung, Art. 16 DSGVO • Recht auf Datenübertragbarkeit, Art. 20 DSGVO • Widerspruchsrecht, Art. 21 DSGVO Es soll sichergestellt sein, dass über das System diese Rechte gewahrt werden können. Eine Auskunft aller relevanten personenbezogenen	☒ Ja, die Anforderung ist umgesetzt durch folgende Maßnahme(n) Die Anforderung ist umgesetzt, da die Date nim System einsehbar sind und bei Anfrage von uns an den Makler übermittelt werden können.

Frage	Erläuterung	Bitte treffen Sie eine Auswahl: Ja oder Nicht anwendbar, weil….. Bitte begründen Sie die jeweilige konkrete Maßnahme. Bei Verweisen auf Dokumentationen fügen Sie diese bitte bei, um die Aussage nachhaltig belastbar zu machen und der Rechenschaftsplicht nachzukommen.
	Daten sollte neben der einfachen Erstellung einer Kopie dieser Daten in einem lesbaren Format möglich sein. Personenbezogene Daten sollen von berechtigten Mitarbeitern einfach aber nachvollziehbar berichtigt werden können. Ein Datenexport in einem maschinenlesbaren Format sollte ebenso möglich sein wie eine Sperrung der Verarbeitung nach erfolgtem Widerspruch.	
I.8 Sind sichere Schnittstellen zur Datenübermittlung vorhanden?	Sofern ein Datenaustausch zwischen dem System und weiteren Systemen gewünscht ist, sollten kompatible Schnittstellen zwischen diesen Systemen vorliegen. Dies soll sicherstellen, dass die personenbezogenen Daten unverfälscht zwischen den Systemen ausgetauscht werden können. Solche Schnittstellen sind allerdings erfahrungsgemäß Angriffspunkte für externe Angreifer. Aus diesem Grund sollten die Schnittstellen derart abgesichert sein, dass ein Datenaustausch nur mit (z.B. über digitale Signaturen) legitimierten Systemen möglich ist und eine dem Schutzbedarf der Daten entsprechende Verschlüsselung des Transportwegs erfolgt.	☒ Ja, die Anforderung ist umgesetzt durch folgende Maßnahme(n) Die Anforderung ist umgesetzt, da Datenübermittlungen ausschließlich über abgesicherte, verschlüsselte Schnittstellen erfolgen.

Frage	Erläuterung	Bitte treffen Sie eine Auswahl: Ja oder Nicht anwendbar, weil….. Bitte begründen Sie die jeweilige konkrete Maßnahme. Bei Verweisen auf Dokumentationen fügen Sie diese bitte bei, um die Aussage nachhaltig belastbar zu machen und der Rechenschaftsplicht nachzukommen.
I.9 Können über die Schnittstellen auch Informationen zur Erfüllung von Betroffenenanfragen weitergegeben werden?	Selbst bei Verwendung eines zentralen Kernbankensystems sind verschiedene personenbezogene Daten oftmals dezentral in unterschiedlichen Systemen gespeichert. Um die Wahrung von Betroffenenrechten hinreichend zu gewährleisten, sollten auch im Rahmen von Betroffenenanfragen personenbezogene Daten aus anderen Systemen abgerufen oder an die relevanten Systeme übermittelt werden können.	☒ Ja, die Anforderung ist umgesetzt durch folgende Maßnahme(n) Die Anforderung ist umgesetzt, da über die Schnittstellen relevante personenbezogene Daten zur Erfüllung von Betroffenenanfragen weitergegeben werden können. (z.b. API)
I.10 Ist die Einhaltung der Grundsatzes des Datenschutzes durch Technikgestaltung vom Hersteller nachweisbar?	Eine Überprüfung der Einhaltung der Grundsätze des Art. 25 DSGVO ist durch den Endanwender in der Regel komplex. Um dennoch eine Nachweisbarkeit herstellen zu können, sollte es alternativ ausreichen, wenn der Hersteller die Datenschutzkonformität durch sonstige Nachweise belegen kann. Ein solcher Nachweis kann durch ein anerkanntes Prüfsiegel, von anerkannten Auditberichten oder auf Basis dieses vollständig ausgefüllten Dokuments erfolgen.	Nachweis erfolgt durch: ☒ Anerkannter Auditbericht (Als Anlage hinzugefügt – Externer Datenschutz Audit, durchgeführt durch eine spezialisierte Rechtsanwaltskanzlei) ☒ Dieses Dokument

Frage	Erläuterung	Bitte treffen Sie eine Auswahl: Ja oder Nicht anwendbar, weil….. Bitte begründen Sie die jeweilige konkrete Maßnahme. Bei Verweisen auf Dokumentationen fügen Sie diese bitte bei, um die Aussage nachhaltig belastbar zu machen und der Rechenschaftsplicht nachzukommen.
I.11 Sind alle Änderungen an Datensätzen nachvollziehbar?	Änderungen an personenbezogenen Daten sollten mit Zeitstempel und Bearbeiterkürzel protokolliert werden, um Manipulationen nachweisen zu können.	☒ Nicht anwendbar, weil Änderungen werden nur für einen begrenzten Zeitraum gespeichert und sind zudem nur eingeschränkt und auf Anfrage einsehbar.
I.12 Werden personenbezogene Daten sicher gespeichert?	Systemrelevante Datenbanken, welche personenbezogene Daten enthalten, sollten mit einem aktuell als sicher anerkannten Algorithmus verschlüsselt werden, um das Risiko eines unberechtigten Zugriffs auf Daten zu verringern.	☒ Ja, die Anforderung ist umgesetzt durch folgende Maßnahme(n) Die Anforderung ist umgesetzt, da personenbezogene Daten in den Datenbanken mit aktuellen, als Sicher anerkannten Verschlüsselungsverfahren gespeichert werden.
II. Data Protection by Default		
II.1 Sind keine vorab verfügbaren Freitextfelder vorhanden?	Es sollten per Voreinstellung keine offenen Freitextfelder vorhanden sein. Sofern Freitextfelder erforderlich sein sollten, sollten diese durch gesondert berechtigte Mitarbeiter und auch nur für den konkreten Anlass freigeschaltet werden können.	☒ Ja, die Anforderung ist umgesetzt durch folgende Maßnahme(n) Die Anforderung ist umgesetzt, da im System keine vorab verfügbaren Freitextfelder vorhanden sind.
II.2 Ist sichergestellt, dass das System keine Daten an den Hersteller bzw. den	Zur Prüfung der Stabilität und Leistungsfähigkeit und zur Durchführung von Supportaufgaben übermitteln verschiedene Systeme dauerhaft personenbezogene Daten	☒ Ja, die Anforderung ist umgesetzt durch folgende Maßnahme(n) Die Anforderung ist umgesetzt, da keine personenbezogenen Daten ohne vorherige Genehmigung an den Hersteller oder Wartungsdienstleister übermittelt werden.

Frage	Erläuterung	Bitte treffen Sie eine Auswahl: Ja oder Nicht anwendbar, weil….. Bitte begründen Sie die jeweilige konkrete Maßnahme. Bei Verweisen auf Dokumentationen fügen Sie diese bitte bei, um die Aussage nachhaltig belastbar zu machen und der Rechenschaftsplicht nachzukommen.
Wartungsdienstleister übermittelt?	wie IP-Adresse oder Benutzerkennungen an den Systemhersteller oder einen beauftragten Wartungsdienstleister. Diese Übermittlungen erfolgen oftmals intransparent für den Endanwender und ohne explizite Rechtsgrundlage. Aus diesem Grund sollte sichergestellt sein, dass solche für die Telemetrie relevanten Daten nur dann an den Hersteller oder einen Wartungsdienstleister übermittelt werden, wenn dies von Seiten des Anwenders bzw. eines Mitarbeiters aus der hauseigenen IT-Abteilung genehmigt worden ist.	
II.3 Ist sichergestellt, dass Remotezugriffe nur anlassbezogen erfolgen können?	Remotezugriffe auf das System sollten nur durch eine aktive Zustimmung des Users möglich sein und dürfen nur so lange aufrechterhalten werden, wie dies für die Remotetätigkeit erforderlich ist. Wird die Verbindung geplant oder ungeplant unterbrochen, sollte eine erneute Zustimmung des Users zum Remotezugriff erforderlich sein.	☒ Ja, die Anforderung ist umgesetzt durch folgende Maßnahme(n) Die Anforderung ist umgesetzt, da Remotezugriffe nur anlassbezogen erfolgen.
II.4 Ist sichergestellt, dass Datenübermittlungen nur erfolgen, wenn der	Übermittlungen personenbezogener Daten an andere Stellen sind nur unter Vorliegen einer	☒ Ja, die Anforderung ist umgesetzt durch folgende Maßnahme(n)

Frage	Erläuterung	Bitte treffen Sie eine Auswahl: Ja oder Nicht anwendbar, weil….. Bitte begründen Sie die jeweilige konkrete Maßnahme. Bei Verweisen auf Dokumentationen fügen Sie diese bitte bei, um die Aussage nachhaltig belastbar zu machen und der Rechenschaftsplicht nachzukommen.
User aktiv zugestimmt hat?	Rechtsgrundlage und eines legitimen Zwecks zulässig. Um sicherzustellen, dass Daten nicht permanent übermittelt werden oder von anderen Systemen abgerufen werden können, sollten Datenübermittlungen nur aktiv durch den User oder einen berechtigten Mitarbeiter angestoßen werden können. Dabei ist es unerheblich, ob es sich um eine einmalige Datenübermittlung oder über eine geplante regelmäßige Datenübermittlung handelt.	Datenübermittlungen erfolgen per Default nur aktiv. Bei vom Kunden selbst eingerichteten APU- oder Webhook-Automatisierungen liegt die Auslösung jedoch außerhalb unseres Einflussbereichs.
II.5 Ist sichergestellt, dass User nur die Benutzerrechte haben, welche sie für ihre Tätigkeit benötigen?	Das Rechte- und Rollenkonzept sollte gewährleisten, dass höherrangige Benutzerrechte nur einem kleinen Personenkreis vorbehalten bleiben (Need-to-know-Prinzip).	☒ Ja, die Anforderung ist umgesetzt durch folgende Maßnahme(n) Die Anforderung ist umgesetzt, da höherrangige Benutzerrechter nur einem eng begrenzten Personenkreis vorbehalten sind.
II.6 Ist sichergestellt, dass bei der Verarbeitung besonders sensitiver Daten höhere Umsicht gewahrt wird?	Bei der Verarbeitung besonders schützenswerter Daten sollte darauf geachtet werden, dass diese Verarbeitung höhere Sicherheitsstandards erfüllt als bei weniger schützenswerten Daten. Dies kann bspw. durch die technische oder organisatorische Umsetzung eines Vier-Augen-Prinzips gewahrt werden.	☒ Ja, die Anforderung ist umgesetzt durch folgende Maßnahme(n) Die Anforderung ist umgesetzt, da besonders sensitive Daten mit erhöhten Sicherheitsstandards verarbeitet werden (s. TOM)

Frage	Erläuterung	Bitte treffen Sie eine Auswahl: Ja oder Nicht anwendbar, weil….. Bitte begründen Sie die jeweilige konkrete Maßnahme. Bei Verweisen auf Dokumentationen fügen Sie diese bitte bei, um die Aussage nachhaltig belastbar zu machen und der Rechenschaftsplicht nachzukommen.
II.7 Ist sichergestellt, dass nur berechtigte Personen mit dem System arbeiten können?	Benutzerkonten sollen personengebunden sein und eine Mehrfaktorautorisierung (z.B. durch Benutzername und Passwort) benötigen, damit sichergestellt ist, dass nur berechtigte Personen Daten verarbeiten können.	☒ Ja, die Anforderung ist umgesetzt durch folgende Maßnahme(n) Die Anforderung ist umgesetzt, da ausschließlich personengebundene Konten mit Passwortschutz verwendet werden und nur berechtigte Personen Zugriff erhalten (Ausnahme durch Kunden eingestelltes SSO)
II.8 Ist die Löschung von personenbezogenen Daten gewährleistet?	Personenbezogene Daten und Belegen sollten nach Ablauf einer festgelegten Löschfrist automatisch gelöscht werden. Ausnahmen von dieser automatisierten Löschung dürfen nur durch berechtigte Benutzer gesondert definiert werden.	☒ Nicht anwendbar, weil Die Löschung erfolgt (noch) nicht automatisiert, sondern muss händisch durch berechtigte Benutzer durchgeführt werden
II.9 Ist sichergestellt, dass die Verarbeitung von personenbezogenen Daten an eine Rechtsgrundlage gebunden ist?	Bestimmte Funktionen der Datenverarbeitungen dürfen nur durchgeführt werden, wenn eine explizite Rechtsgrundlage zur Datenverarbeitung (z.B. in Form einer Kundeneinwilligung) gegeben ist. Ansonsten sind die entsprechenden Datensätze für diese Funktionen gesperrt und können auch im Rahmen von Stapelverarbeitung nicht verwendet werden.	☒ Ja, die Anforderung ist umgesetzt durch folgende Maßnahme(n) Die Anforderung ist umgesetzt, da personenbezogene Daten ausschließlich auf Basis einer gültigen Rechtsgrundlage verarbeitet werden,

Frage	Erläuterung	Bitte treffen Sie eine Auswahl: Ja oder Nicht anwendbar, weil….. Bitte begründen Sie die jeweilige konkrete Maßnahme. Bei Verweisen auf Dokumentationen fügen Sie diese bitte bei, um die Aussage nachhaltig belastbar zu machen und der Rechenschaftsplicht nachzukommen.
II.10 Ist die Einhaltung der Grundsatzes des Datenschutzes durch datenschutzfreundliche Voreinstellungen vom Hersteller nachweisbar?	Eine Überprüfung der Einhaltung der Grundsätze des Art. 25 DSGVO ist durch den Endanwender in der Regel komplex. Um dennoch eine Nachweisbarkeit herstellen zu können, sollte es alternativ ausreichen, wenn der Hersteller die Datenschutzkonformität durch sonstige Nachweise belegen kann. Ein solcher Nachweis kann durch ein anerkanntes Prüfsiegel, von anerkannten Auditberichten oder auf Basis dieses vollständig ausgefüllten Dokuments erfolgen.	Nachweis erfolgt durch: ☒ Anerkannter Auditbericht Die Anforderung ist umgesetzt, da jährliche Datenschutz-Audits durch einen spezialisierten Rechtsanwalt die datenschutzfreundlichen Voreinstellungen nachweisbar bestätigen. ☒ Dieses Dokument

Die datenschutzrechtlichen Anforderungen gem. I. Data Protection by Design und II. Data Protection by Default sind eingehalten

Köln, den 14.04.2026

Ort / Datum **Unterschrift / Funktion / Stempel**