Es handelt sich hierbei nur um einen Entwurf. Das unterschriftsreife Dokument erhalten Sie bei Ihrem Kundenbetreuer.

Vertrag über Auftragsverarbeitung

im Sinne von Art. 28 Abs. 3 DSGVO

zwischen

Firma
Straße
Ort
- im Folgenden: Auftraggeber -

und

Flowmium GmbH
Robert-Bosch-Str. 7
64293 Darmstadt
- im Folgenden: Auftragnehmer -

1. Allgemeine Bestimmungen und Vertragsgegenstand

1.1 Gegenstand des vorliegenden Vertrags ist die Verarbeitung personenbezogener Daten im Auftrag durch den Auftragnehmer (Art. 28 DSGVO). Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO ist der Auftraggeber. Die Auftragsdetails entnehmen Sie der Anlage 1.

1.2 Die Verarbeitung der vertragsgegenständlichen personenbezogenen Daten außerhalb der Europäischen Union ist nur zulässig, wenn die gesetzlichen Voraussetzungen der Art. 44 ff. DSGVO gegeben sind und der Auftraggeber zugestimmt hat.

2. Vertragslaufzeit und Kündigung

2.1 Die Laufzeit des vorliegenden Vertrags richtet sich nach der Laufzeit des Hauptvertrags (Angebotsannahme). Findet nach Beendigung des Hauptvertrags weiterhin eine Auftragsverarbeitung statt, gilt dieser Vertrag für die betreffenden Verarbeitungsvorgänge fort. Eine ordentliche, vom Hauptvertrag unabhängige Kündigung des vorliegenden Vertrags ist unzulässig. Das Recht zur außerordentlichen fristlosen Kündigung aus wichtigem Grund bleibt unberührt.

3. Weisungen des Auftraggebers

3.1 Der Auftragnehmer darf Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Auftraggebers erheben, nutzen oder auf sonstige Weise verarbeiten, insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Wird der Auftragnehmer durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit. Der Auftragnehmer informiert den Auftraggeber unverzüglich, falls er der Auffassung ist, dass eine Weisung des Auftraggebers gegen gesetzliche Vorschriften verstößt. Wird eine Weisung erteilt, deren Rechtmäßigkeit der Auftragnehmer substantiiert anzweifelt, ist der Auftragnehmer berechtigt, deren Ausführung vorübergehend auszusetzen, bis der Auftraggeber diese nochmals ausdrücklich bestätigt oder ändert. Besteht die Möglichkeit, dass der Auftragnehmer durch das Befolgen der Weisung einem Haftungsrisiko ausgesetzt wird, kann die Durchführung der Weisung bis zur Klärung der Haftung im Innenverhältnis ausgesetzt werden. Ist eine Verarbeitung aufgrund zwingenden Rechts erforderlich, teilt der Auftragnehmer dies dem Auftraggeber vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

3.2 Weisungen sind grundsätzlich schriftlich oder in einem elektronischen Format (z. B. per E-Mail) zu erteilen. Mündliche Weisung sind in begründeten Einzelfällen zulässig und werden vom Auftraggeber unverzüglich schriftlich oder in einem elektronischen Format bestätigt. In der Bestätigung ist ausdrücklich zu begründen, warum keine schriftliche Weisung erfolgen konnte. Der Auftragnehmer hat Person, Datum und Uhrzeit der mündlichen Weisung in angemessener Form zu protokollieren.

3.3 Der Auftraggeber benennt auf Verlangen des Auftragnehmers in Anlage 3 eine oder mehrere weisungsberechtigte Personen. Personelle Änderungen sind dem Auftragnehmer unverzüglich mitzuteilen.

4. Kontrollbefugnisse des Auftraggebers

4.1 Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

4.2 Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

4.3 Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren); oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

5. Allgemeine Pflichten des Auftragnehmers

5.1 Die Verarbeitung der vertragsgegenständlichen Daten durch den Auftragnehmer erfolgt ausschließlich auf Grundlage der vertraglichen Vereinbarungen in Verbindung mit den ggf. erteilten Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung ist nur aufgrund zwingender europäischer oder mitgliedsstaatlicher Rechtsvorschriften zulässig (z. B. im Falle von Ermittlungen durch Strafverfolgungs- oder Staatsschutzbehörden).

5.2 Der Auftragnehmer hat zu gewährleisten, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO). Vor der Unterwerfung unter die Verschwiegenheitspflicht dürfen die betreffenden Personen keinen Zugang zu den vom Auftraggeber überlassenen personenbezogenen Daten erhalten.

6. Technische und organisatorische Maßnahmen

6.1 Der Auftragnehmer hat geeignete technische und organisatorische Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus festgelegt und diese in Anlage 2 dieses Vertrags dokumentiert. Die dort beschriebenen Maßnahmen wurden unter Beachtung der Vorgaben von Art. 32 DSGVO ausgewählt. Der Auftragnehmer wird die technischen und organisatorischen Maßnahmen bei Bedarf und / oder anlassbezogen überprüfen und anpassen, mindestens jedoch alle 2 Jahre.

7. Unterstützungspflichten des Auftragnehmers

7.1 Der Auftragnehmer wird den Auftraggeber gem. Art. 28 Abs. 3 lit. e DSGVO bei dessen Pflichten zur Wahrung der Betroffenenrechte aus Kapitel III, Art. 12 – 22 DSGVO, unterstützen. Dies gilt insbesondere für die Erteilung von Auskünften und die Löschung, Berichtigung oder Einschränkung personenbezogener Daten. Der Auftragnehmer wird den Auftraggeber ferner gem. Art. 28 Abs. 3 lit. f DSGVO bei dessen Pflichten nach Art. 32 – 36 DSGVO (insb. Meldepflichten) unterstützen. Die Reichweite dieser Unterstützungspflichten bestimmt sich im Einzelfall unter Berücksichtigung der Art der Verarbeitung und der Informationen, die dem Auftragnehmer zur Verfügung stehen. Der Auftraggeber kann eine Unterstützung beim Auftragnehmer schriftlich oder in Textform bei den in der Anlage 3 genannten Personen anfordern. Der Auftragsnehmer stellt dem Auftraggeber die Meldung schriftlich oder in Textform zu.

8. Einsatz von Unterauftragsverarbeitern

8.1 Der Auftragnehmer ist zum Einsatz von Unterauftragsverarbeitern (Subunternehmern) berechtigt. Alle zum Zeitpunkt des Vertragsschlusses bereits bestehenden Subunternehmerverhältnisse des Auftragnehmers sind diesem Vertrag abschließend in Anlage 1 beigefügt. Für die in Anlage 1 aufgezählten Subunternehmer gilt die Zustimmung mit Abschluss dieses Vertrags als erteilt.

8.2 Beabsichtigt der Auftragnehmer den Einsatz weiterer Subunternehmer, wird er dies dem Auftraggeber rechtzeitig - spätestens jedoch zwei Wochen - vor deren Einsatz in schriftlicher oder elektronischer Form anzeigen. Der Auftraggeber hat nach dieser Mitteilung zwei Wochen Zeit, der Hinzuziehung des / der Subunternehmer zu widersprechen. Erfolgt innerhalb dieser Frist kein Widerspruch, gilt die Hinzuziehung des / der Subunternehmer(s) als genehmigt. Im Falle eines Widerspruchs dürfen die betroffenen Subunternehmer nicht eingesetzt werden. Widersprüche sind nur zulässig, wenn der Auftraggeber begründete Anhaltspunkte dafür hat, dass durch den Einsatz des Unterauftragnehmers die Datensicherheit oder der Datenschutz eingeschränkt würde, die Einhaltung gesetzlicher oder vertraglicher Bestimmungen gefährdet wäre und / oder sonstige berechtigte Interessen des Auftraggebers entgegenstehen; die entsprechenden Verdachtsmomente sind dem Widerspruch beizufügen.

8.3 Subunternehmer werden vom Auftragnehmer unter Beachtung der gesetzlichen und vertraglichen Vorgaben ausgewählt. Sämtliche Verträge zwischen Auftragsverarbeiter und Unterauftragsverarbeiter (Subunternehmerverträge) müssen den gesetzlichen Vorschriften über die Verarbeitung personenbezogener Daten im Auftrag genügen; dies betrifft insbesondere die Implementierung geeigneter technischer und organisatorischer Maßnahmen nach Art. 32 DSGVO im Betrieb des Subunternehmers. Nebenleistungen, welche der Auftragnehmer zur Ausübung seiner geschäftlichen Tätigkeit in Anspruch nimmt, stellen keine Unterauftragsverhältnisse im Sinne des Art. 28 DSGVO dar. Nebentätigkeiten in diesem Sinne sind insbesondere Telekommunikationsleistungen ohne konkreten Bezug zur Hauptleistung, Post- und Transportdienstleistungen, Wartung und Benutzerservice sowie sonstige Maßnahmen, die die Vertraulichkeit und / oder Integrität der Hard- und Software sicherstellen sollen und keinen konkreten Bezug zur Hauptleistung aufweisen. Der Auftragnehmer wird jedoch auch bei diesen Drittleistungen die Einhaltung der gesetzlichen Datenschutzstandards (insbesondere durch entsprechende Vertraulichkeitsvereinbarungen) sicherstellen. Der Auftraggeber führt regelmäßig, mindestens jedoch alle 2 Jahre, ein Überprüfung der Subunternehmer durch. Das beinhaltet insbesondere die Überprüfung der technischen und organisatorischen Maßnahmen sowie der Aktualität der Zertifikate (z.B. ISO 27001).

8.4 Sämtliche Verträge zwischen dem Auftragnehmer und dem Unterauftragsverarbeiter (Subunternehmerverträge) müssen den Anforderungen dieses Vertrags und den gesetzlichen Vorschriften über die Verarbeitung personenbezogener Daten im Auftrag genügen.

8.5 Die Beauftragung von Subunternehmern in Drittstaaten ist nur zulässig, wenn die gesetzlichen Voraussetzungen der Art. 44 ff. DSGVO gegeben sind und der Auftraggeber zugestimmt hat.

9. Mitteilungspflichten des Auftragnehmers

9.1 Verstöße gegen diesen Vertrag, gegen Weisungen des Auftraggebers oder gegen sonstige datenschutzrechtliche Bestimmungen sind dem Auftraggeber unverzüglich mitzuteilen; das gleiche gilt bei Vorliegen eines entsprechenden begründeten Verdachts. Diese Pflicht gilt unabhängig davon, ob der Verstoß vom Auftragnehmer selbst, einer bei ihm angestellten Person, einem Unterauftragsverarbeiter oder einer sonstigen Person, die er zur Erfüllung seiner vertraglichen Pflichten eingesetzt hat, begangen wurde.

9.2 Ersucht ein Betroffener, eine Behörde oder ein sonstiger Dritter den Auftragnehmer um Auskunft, Berichtigung, Einschränkung der Verarbeitung oder Löschung, wird der Auftragnehmer die Anfrage unverzüglich an den Auftraggeber weiterleiten; in keinem Fall wird der Auftragnehmer dem Ersuchen des Betroffenen ohne Weisung / Zustimmung des Auftraggebers nachkommen.

9.3 Der Auftragnehmer wird den Auftraggeber unverzüglich informieren, wenn Aufsichtshandlungen oder sonstige Maßnahmen einer Behörde bevorstehen, von der auch die Verarbeitung, Nutzung oder Erhebung der durch den Auftraggeber zur Verfügung gestellten personenbezogenen Daten betroffen sein könnten. Darüber hinaus hat der Auftragnehmer den Auftraggeber unverzüglich über alle Ereignisse oder Maßnahmen Dritter zu informieren, durch welche die vertragsgegenständlichen Daten gefährdet oder beeinträchtigt werden könnten.

10. Vertragsbeendigung, Löschung und Rückgabe der Daten

10.1 Nach Abschluss der vertragsgegenständlichen Datenverarbeitung bzw. nach Beendigung dieses Vertrags hat der Auftragnehmer alle personenbezogenen Daten nach Wahl des Auftraggebers zu löschen oder zurückzugeben, sofern keine rechtliche oder vertragliche Verpflichtung zur Speicherung der betreffenden Daten mehr besteht (z. B. gesetzliche Aufbewahrungsfristen).

11. Datengeheimnis und Vertraulichkeit

11.1 Der Auftragnehmer ist unbefristet und über das Ende dieses Vertrages hinaus verpflichtet, die im Rahmen der vorliegenden Vertragsbeziehung erlangten personenbezogenen Daten vertraulich zu behandeln. Der Auftragnehmer verpflichtet sich, seine Mitarbeiter mit den einschlägigen Datenschutzbestimmungen und Geheimnisschutzregeln vertraut zu machen und sie zur Verschwiegenheit zu verpflichten, bevor diese ihre Tätigkeit beim Auftragnehmer aufnehmen.

12. Schlussbestimmungen

12.1 Änderungen dieses Vertrags und Nebenabreden bedürfen der schriftlichen oder elektronischen Form, die eindeutig erkennen lässt, dass und welche Änderung oder Ergänzung der vorliegenden Bedingungen durch sie erfolgen soll.

12.2 Sollte sich die DSGVO oder sonstige in Bezug genommenen gesetzlichen Regelungen während der Vertragslaufzeit ändern, gelten die hiesigen Verweise auch für die jeweiligen Nachfolgeregelungen.

12.3 Sollten einzelne Teile dieser Vereinbarung unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen hiervon unberührt.

12.4 Sämtliche Anlagen zu diesem Vertrag sind Vertragsbestandteil.

12.5 Sind die Vertragsparteien Kaufleute, juristische Personen des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen, ist der Sitz des Auftragnehmers Gerichtsstand für alle Streitigkeiten aus diesem Vertrag, sofern insoweit hierfür ein ausschließlicher Gerichtsstand nicht begründet wird.

flowmium

Auftragnehmer	Auftraggeber
Robert Lassen, Geschäftsführer	
_____	_____
Ansprechpartner und Position	Ansprechpartner und Position
_____	_____
Datum, Unterschrift	Datum, Unterschrift

Anlage 1 zum Vertrag über Auftragsverarbeitung

Auftragsdetails und Subunternehmer

Gegenstand des Auftrags

Der vorliegende Vertrag umfasst, im Zusammenhang mit dem Hauptvertrag, die Verarbeitung personenbezogener Daten im Zusammenhang mit der Nutzung der Software „Flowmium Zeugnisgenerator".

Zweck der Datenverarbeitung

Der Zweck des Flowmium Zeugnisgenerators ist die Erstellung von Arbeitszeugnissen inkl. der Abbildung des Workflows zur Beantragung und Bearbeitung durch Mitarbeiter und Vorgesetzte.

Art der Daten/Datenkategorien

Im Rahmen der vertraglichen Leistungserbringung werden regelmäßig folgende Datenarten verarbeitet:

- Persönliche Daten (Anrede, Vorname, Nachname, Titel/akademischer Grad, Geburtsdatum, Geburtsort)
- Kontaktdaten (Straße, Postleitzahl, Ort, E-Mail-Adresse)
- Beschäftigungsdaten (Eintrittsdatum, Austritts-/Ausstellungsdatum, Austritts-/Ausstellungsgrund, Tätigkeitsbeschreibungen, Unterbrechungen, Vollmachten)
- Zeugnisbewertungen (Bereitschaft, Befähigung, Wissen, Weiterbildung, Arbeitsweise, Arbeitserfolg, Führungserfolg, Verhalten Intern, Verhalten Extern, Ergebnis Abschlussprüfung, diverse persönliche und fachliche Attribute)
- Erstellte Arbeitszeugnisse

Kreis der Betroffenen

Bei dem Kreis der von der Datenverarbeitung betroffenen Personen handelt es sich um:

- Beschäftigte und ehemalige Beschäftigte des Auftraggebers

flowmium

Art der Datenverarbeitung

Es werden vom Auftragnehmer Daten

- erhoben / erfasst
- gespeichert
- gelöscht (je nach Einstellung; nach Vertragsende)
- ausgelesen / abgefragt (nur bei Schnittstelle zu einem HR-System)

Liste der bestehenden Subunternehmer zum Zeitpunkt des Vertragsschlusses

(Unternehmens-) Name und Anschrift	Ort der Leistungserbringung	Leistung
centron GmbH Heganger 29 96103 Hallstadt	96103 Hallstadt, Deutschland	Hosting der Anwendung einschl. Backups und Patch-Management im Rahmen eines Managed Services

Kontaktdaten des Datenschutzbeauftragten

York Hoffmann
Robin Data GmbH
Fritz-Haber-Str. 9
06217 Merseburg
E-Mail: dsb@robin-data.io
Telefon: 03461 – 479236-0

Ansprechpartner beim Auftragnehmer:

Name:	Robert Lassen
Position:	Geschäftsführer
Telefon:	[nicht im Web zu sehen]
E-Mail:	[nicht im Web zu sehen]

Anlage 2 zum Vertrag über Auftragsverarbeitung

Technische und organisatorische Maßnahmen (TOM) im Sinne von Art. 32 DSGVO

Flowmium GmbH
Robert-Bosch-Str. 7
64293 Darmstadt

Allgemeines

Die Flowmium GmbH betreibt keine eigenen Datenverarbeitungsanlagen. Kundendaten werden im Rechenzentrum der centron GmbH in Hallstadt (Deutschland) gespeichert und verarbeitet. Wir verweisen auf die technischen und organisatorischen Maßnahmen der centron GmbH, die diesem Dokument beiliegen.

Flowmium betreibt ein ISMS nach ISO 27001 und ist seit dem 18.01.2024 zertifiziert.

1. Vertraulichkeit

1.1. Zutrittskontrolle

Flowmium stellt sicher, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Dies geschieht durch:

Technische Maßnahmen	Organisatorische Maßnahmen
Elektronisches Türschloss zum Büro	Protokollierte Schlüsselverwaltung
Abschließbare Fenster im Erdgeschoss	Dokumentierte Sicherheitsverfahren für Büros sowie sichere Bereiche und Betriebsmittel

1.2. Zugangskontrolle

Flowmium verhindert, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können. Dies geschieht durch:

Technische Maßnahmen	Organisatorische Maßnahmen
Login mit Benutzername + Passwort	Anweisung zur Sperrung des PCs beim Verlassen des Arbeitsplatzes
2-Faktor-Authentifizierung zu Server-, E-Mail- und Dokumentensystemen. Bei allen anderen Anwendungen, wenn möglich.	Automatische Sperre des PCs bei Inaktivität
Anti-Viren-Software auf PCs/Notebooks	Definierter Ablauf zur Löschung der Berechtigungen von ausgeschiedenen Mitarbeitern
Verschlüsselung von PCs/Notebooks	
Verschlüsselung von Smartphones	
Einsatz von Firewall und regelm. Aktualisierung	

1.3. Zugriffskontrolle

Flowmium gewährleistet, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Dies geschieht durch:

Technische Maßnahmen	Organisatorische Maßnahmen
Verschlüsselung der Datenbanken auf Dateiebene per TDE. Verschlüsselungsalgorithmus: AES256	Einsatz eines Berechtigungskonzepts
Aktenvernichter mit geeigneter Sicherheitsstufe	Minimale Anzahl an Administratoren
	Vergabe minimaler Berechtigungen
	Vernichtung von Datenträgern gemäß Entsorgungskonzept

1.4. Trennungskontrolle

Flowmium gewährleistet, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dies geschieht durch:

Technische Maßnahmen	Organisatorische Maßnahmen
Logische Trennung der personenbezogenen Daten für unterschiedliche Auftraggeber	
Trennung von Produktiv- und Testsystem	
Steuerung über Berechtigungskonzept	

2. Integrität

2.1. Weitergabekontrolle

Flowmium gewährleistet, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. Dies geschieht durch:

Technische Maßnahmen	Organisatorische Maßnahmen
Bereitstellung der Website und App über verschlüsselte Verbindungen (https)	Ordnungsgemäße Vernichtung von Datenträgern
Stellung von Hard- und Software für den Home-Office Arbeitsplatz	
Zugang zu Servern (Applikation und Datenbank) nur über VPN möglich	

2.2. Eingabekontrolle

Flowmium gewährleistet, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Dies geschieht durch:

Technische Maßnahmen	Organisatorische Maßnahmen
Protokollierung der Eingabe, Änderung und Löschung von Daten	
Protokollierung der Eingabe, Änderung und Löschung von personenbezogenen Daten nach Benutzer in der Anwendung	

Vergabe von rollenbasierten Berechtigungen in der Anwendung	

3. Verfügbarkeit und Belastbarkeit

3.1. Verfügbarkeitskontrolle

Flowmium gewährleistet, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Dies geschieht durch:

Technische Maßnahmen	Organisatorische Maßnahmen
Datensicherung mehrmals täglich	Backup & Recovery-Konzept
	Regelmäßig Überprüfung der Backups und Tests auf Wiederherstellbarkeit

3.2. Belastbarkeit

Flowmium gewährleistet die Belastbarkeit der Systeme und Dienste. Dies geschieht durch:

Technische Maßnahmen	Organisatorische Maßnahmen
Einrichtung von Warnregeln zur Erkennung einer erhöhten Serverauslastung	Regelmäßige Überprüfung der Serverauslastung und Anpassung der Kapazitäten

3.3. Wiederherstellbarkeit

Flowmium gewährleistet die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu diesen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen. Dies geschieht durch:

Technische Maßnahmen	Organisatorische Maßnahmen
Regelmäßige Backups der Datenbanken	Backup & Recovery-Konzept
	Regelmäßige Überprüfung der Backups und Test auf Wiederherstellbarkeit

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

4.1. Datenschutz-Management

Technische Maßnahmen	Organisatorische Maßnahmen
Software-Lösungen für Datenschutz-Management im Einsatz	Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mind. Jährlich durchgeführt
	Mitarbeiter geschult und auf Vertraulichkeit / Datengeheimnis verpflichtet
	Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach
	Regelmäßige Datenschutzaudits

4.2. Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen.

Technische Maßnahmen	Organisatorische Maßnahmen
Einsatz von Firewall und regelmäßige Aktualisierung	Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Daten-Pannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
Einsatz von Spamfilter und regelmäßige Aktualisierung	Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen
Einsatz von Virenscanner und regelmäßige Aktualisierung	

4.3. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Privacy by design / Privacy by default

Technische Maßnahmen	Organisatorische Maßnahmen
Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	

Es werden datenschutzfreundliche Voreinstellungen (Privacy by default) gewählt.	
Die Anwendung wurde/wird nach dem aktuellen Stand der Technik entwickelt und weiterentwickelt (Privacy by design).	

4.4. Auftragskontrolle

Flowmium gewährleistet, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Dies geschieht durch:

Technische Maßnahmen	Organisatorische Maßnahmen
	Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
	Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit)
	Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standard-Vertragsklauseln
	Schriftliche Weisungen an den Auftragnehmer

Technische und organisatorische Maßnahmen der centron GmbH

centron®

Technische und organisatorische Maßnahmen gemäß Artikel 32 DSGVO

Beschreibung der technischen und organisatorischen Maßnahmen

(Art. 32 Abs. 1 lit. d, Art 15 Abs. 1 DS-GVO)

Allgemeine Maßnahmen

- Auf Basis der ISO 27001 wird ein ISMS betrieben
  - Erstzertifizierung 04.04.2020
  - Gültigkeitsdauer 04.07.2026
- TrustedCloud Zertifizierung, 14.06.2014
- Die Informationssicherheits-, IT-Nutzungs- und Datenschutzrichtlinie ist für alle Mitarbeiter im Zugriff und wird regelmäßig oder bei Bedarf aktualisiert
- Ein Datenschutzbeauftragter ist gestellt und der Geschäftsführung direkt unterstellt
- Ein Risikomanagement ist etabliert und berichtet an die Geschäftsführung
- Eine Notfallplanung und ein Wiederanlaufplan ist etabliert
- Ein Incidentmanagement-System ist etabliert
- Alle Mitarbeiter werden auf die Einhaltung des Datenschutzes und Verschwiegenheit verpflichtet

Trusted Cloud SERVICE 10010

Information Security Management System ISO 27001 Zertifiziert

Testat IT-Grundschutz Basis-Absicherung IGT-0001-2021 centron GmbH Bundesamt für Sicherheit in der Informationstechnik

centron GmbH
Heganger 29
96103 Hallstadt

Telefon **+49 (0)951 968 34 0**
Telefax **+49 (0)951 968 34 29**
www.centron.de • info@centron.de

USt-IdNr **DE205074466**
Amtsgericht Bamberg
HRB 3986

Geschäftsführer:
Dipl.-Kffr. Monika Seucan
Wilhelm Seucan

Vertraulichkeit

Zutrittskontrolle

Maßnahmen, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren:

- Zugangskontrollsystem
  - Türsicherung im Bürogebäude (elektrische Türöffner mit Zugriffsprotokollierung sowie protokollierte Schlüsselvergabe gemäß Schlüsselmanagement).
  - Zusätzliche biometrische Zugangssicherung zum Rechenzentrum und elektronische Türsicherung zwecks zweistufiger Zutrittskontrolle.
- Einrichtung von Schutzzonen und Festlegung von Zutrittsregeln
- Besucherregelung
  - Protokollierung sämtlicher Besucher
  - Besuche und Lieferanten unterliegen in Abhängigkeit der Schutzzone einer durchgängigen Aufsicht.
- Rundum Videoüberwachung des Gebäude-Außenbereichs mit Sabotageerkennung und Aufzeichnung. Lückenlose Videoüberwachung des Rechenzentrum-Innenbereichs.
- Einbruchmeldeanlage mit Aufschaltung des Sicherheitsdienstes.

Zugangskontrolle

Maßnahmen, um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

- Erteilung von Berechtigungen nach dem Rollen- und Berechtigungskonzept nach Notwendigkeit
- Festlegung von Berechtigungen durch Leitung der Technik und Geschäftsführung
- Protokollierte Vergabe von Berechtigungen durch die Leitung der Technik
- Arbeitsplatz-PCs sind durch lokale Passwörter der Mitarbeiter geschützt
- Im Intranet werden Passwortrichtlinien durch MS-AD umgesetzt (u.a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennworts)
- Die lokalen Systeme der Mitarbeiter werden regelmäßig bei Erscheinen von Updates aktualisiert
- Automatische Sperrung (z.B. Kennwort oder Pausenschaltung)
- Vorschaltung einer physikalischen Firewall mit IDS und IPS
- Einsatz von Virenscannern
- Physikalische Trennung von Netzwerken
- Überwachung des Netzwerktraffics

centron GmbH
Heganger 29
96103 Hallstadt

Telefon **+49 (0)951 968 34 0**
Telefax **+49 (0)951 968 34 29**
www.centron.de • info@centron.de

USt-IdNr **DE205074466**
Amtsgericht Bamberg
HRB 3986

Geschäftsführer:
Dipl.-Kffr. Monika Seucan
Wilhelm Seucan

Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

- Die Passwortvergabe erfolgt ausschließlich durch berechtigtes Personal an vom Auftraggeber benannte Personen
- Die Weisungskommunikation erfolgt auf Seiten des Auftragnehmers über ein ITIL-konformes Ticketsystem
- Die Berechtigung zur Datenverarbeitung personenbezogener Daten werden durch das Active-Directory gesteuert und protokolliert
- Protokollierung der Logins auf den Systemen
- Vernichtung von Datenträgern gemäß Datenträgervernichtungskonzept
- Sofern der Kunde auf seinen Systemen personenbezogene Daten verarbeitet, ist der Kunde primär selbst für die Absicherung der Daten zuständig. Wird diese Zuständigkeit abgetreten, so sind die Sicherungsmechanismen vom Kunden in unregelmäßigen Abständen zu überprüfen und gegebenenfalls zu bemängeln.

Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

- Sämtliche Daten können aufgrund der Art ihrer Speicherung getrennt voneinander verarbeitet werden
- Ausschließliche Verwendung von Software, die eine Mandantenfähigkeit bereitstellt
- Trennung der verarbeitenden Systeme
- Trennung der Systeme in Produktiv- und Testumgebung
- Kunden haben gegenseitig keinen Zugriff auf andere Kundensysteme

Integrität

Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transportes oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

- Eine Weitergabe von personenbezogenen Daten erfolgt nur auf Verlangen von berechtigten Personen oder Institutionen

centron GmbH
Heganger 29
96103 Hallstadt

Telefon **+49 (0)951 968 34 0**
Telefax **+49 (0)951 968 34 29**
www.centron.de • info@centron.de

USt-IdNr **DE205074466**
Amtsgericht Bamberg
HRB 3986

Geschäftsführer:
Dipl.-Kffr. Monika Seucan
Wilhelm Seucan

- Sofern eine Übertragung von personenbezogene Daten an berechtigte Personen oder Institutionen stattfindet, erfolgt diese verschlüsselt, auf ausdrücklichen Kundenwunsch auch unverschlüsselt

Datenträger, die personenbezogene Daten enthalten, werden bei einer Entsorgung des Datenträgers mehrfach durch unterschiedliche Löschmethoden bereinigt, anschließend wird der Datenträger zerstört und ordnungsgemäß entsorgt

Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

- Protokollierung der Systemaktivitäten durch ein Monitoringsystem
- Teilautomatisierte Auswertung von Logdateien
- Protokollierung aller Arbeiten in ITIL-konformem Ticketsystem
- Neue personenbezogene Daten können nur von berechtigten Personen eingegeben werden

Zugriffe auf das Datenverarbeitungssystem werden (siehe Punkt Zugriffskontrolle) protokolliert.

Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- RAID (redundante Datenschreibung auf Festplatten)
- Sicherungskopien werden, falls durch Auftraggeber beauftragt, in Form von Backups gemäß Backupkonzept erstellt
- Rhythmus: täglich oder nach Kundenwunsch
- Aufbewahrungszeit: redundant, 1-5 Wochen oder nach Kundenwusch
- Dateiformat: binär, proprietär verschlüsselt
- Aufbewahrungsort ist, je nach Auftrag, dedizierte Storage- oder Serversysteme des Auftraggebers im eigenen oder fremden Rechenzentrum oder globale Storagesysteme des Auftragnehmers, welche wiederum interne Fehlertoleranz aufweisen und mit Zugangskontrollen versehen sind
- Je nach Auftrag durch den Auftraggeber: Konfiguration der Serversysteme mit Hardware-RAID (Spiegelung der Festplatten), redundante Netzteile
- Regelmäßige Prüfung der Backups auf Funktionalität
- Umsetzung von Disaster und Recovery Konzept, Notfallkonzept und Wiederanlaufplan

centron GmbH
Heganger 29
96103 Hallstadt

Telefon **+49 (0)951 968 34 0**
Telefax **+49 (0)951 968 34 29**
www.centron.de • info@centron.de

USt-IdNr **DE205074466**
Amtsgericht Bamberg
HRB 3986

Geschäftsführer:
Dipl.-Kffr. Monika Seucan
Wilhelm Seucan

Rechenzentrum: Unterbrechungsfreie Stromversorgung (USV), Notstrom-Dieselanlage, redundante Klimaversorgung, Brandfrüherkennungsanlage, regelmäßige Brandbekämpfungsschulungen der Mitarbeiter

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Datenschutzmanagement

- Jährliche Überprüfung der Risikoabschätzung für die Verarbeitung personenbezogener Daten
- Jährliche Prüfung der technischen und organisatorischen Maßnahmen auf Angemessenheit und Stand der Technik
- Führen eines zentralen Datenschutzmanagementsystems
- Regelmäßige interne Datenschutz-Audits
- Regelmäßige Schulungen und Sensibilisierungsmaßnahmen zu den Themen Datenschutz und Informationssicherheit

Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle)

- Aufträge durch Kunden die eine Verarbeitung von personenbezogenen Daten verlangen, werden in einem Ticketsystem protokolliert, für das Ticketsystem ist eine Zugriffskontrolle konfiguriert
- Aufträge sind elektronisch nur von verifizierten Kontaktadressen möglich (Email und Fax)
- Aufträge sind ebenfalls per Post in Schriftform nur durch verifizierte Adressen möglich
- Personen, die Aufträge erteilen, müssen vom Vertragspartner für die Erteilung von Aufträgen autorisiert worden sein

centron GmbH
Heganger 29
96103 Hallstadt

Telefon **+49 (0)951 968 34 0**
Telefax **+49 (0)951 968 34 29**
www.centron.de • info@centron.de

USt-IdNr **DE205074466**
Amtsgericht Bamberg
HRB 3986

Geschäftsführer:
Dipl.-Kffr. Monika Seucan
Wilhelm Seucan

Zertifikate

Zertifikat

Prüfungsnorm **ISO/IEC 27001:2022**

Zertifikat-Registrier-Nr. **01 153 2300399**

Unternehmen:

flowmium

Flowmium GmbH
Robert-Bosch-Str. 7
64293 Darmstadt
Deutschland

Geltungsbereich: Entwicklung, Betrieb und Vertrieb von Unternehmenssoftware für den Bereich Personal.

SoA Version 1.1 vom 18.11.2023

Durch ein Audit wurde der Nachweis erbracht, dass die Forderungen der ISO/IEC 27001:2022 erfüllt sind.

Gültigkeit: Dieses Zertifikat ist gültig vom 18.01.2024 bis 17.01.2027.
Erstzertifizierung 2024

29.01.2024

TÜV Rheinland Cert GmbH
Am Grauen Stein · 51105 Köln

www.tuv.com

IAF MEMBER OF MULTILATERAL RECOGNITION ARRANGEMENT

DAkkS Deutsche Akkreditierungsstelle D-ZM-16031-01-00

TÜVRheinland®
Genau. Richtig.

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-IGZ-0555-2023

ISO 27001-Zertifikat auf der Basis von IT-Grundschutz

Prozess Hosting

der centron GmbH

gültig bis: 4. Juli 2026*

Der Prozess Hosting beinhaltet folgende Teilbereiche: Der Betrieb des Rechenzentrums am Standort Hallstadt und der dazu notwendigen Infrastruktur. Unter der Bereitstellung von Rackspace für Kunden. wird die Zurverfügungstellung von Einbauplätzen verstanden. Die centron GmbH stellt das dazu notwendige Rechenzentrum zur Verfügung und betreibt dies. Ebenso wird Strom und ein Netzwerkanschluss bereitgestellt. Seitens der centron GmbH wird die Hardware optional auf Kundenwunsch auf Funktionsfahigkeit überwacht. Bei Defekten werden auf Wunsch des Kunden Hardwarekomponenten ausgetauscht. Weitere IT-Service-Leistungen sind nicht Teil der Bereitstellung von Rackspace. Die Bereitstellung von Servern für Kunden beinhaltet den Betrieb des Rechenzentrums und die Installation, sowie den Betrieb von Serverhardware. Zusätzlich das Monitoring der genannten Serverhardware. Nicht Teil der Bereitstellung von Servern sind die auf den Servern installierten virtuellen Umgebungen, die Betriebssysteme und die installierten Kundenapplikationen. Für diese sind die Kunden vollständig selbst verantwortlich. Der Prozess des Dienstleister-Managements gliedert sich in die Teilbereiche Auswahl, Beauftragung und Überwachung. Zu den relevanten Dienstleistern zählen solche Dienstleister, die Support für die genannten Tätigkeiten und Leistungen der centron GmbH erbringen. Dazu zählen auch insbesondere solche Dienstleister, bei denen Rackspace seitens der centron GmbH angemietet wird. Nicht Teil des Informationsverbundes sind Dienstleister, die Dienstleistungen für die virtuelle Umgebung, Betriebssysteme und Anwendungen der Kunden erbringen. Alle anderen Prozessabläufe der centron GmbH sind nicht Teil des Informationsverbundes.

Der oben aufgeführte Untersuchungsgegenstand wurde von Auditteamleiter Frank-Stefan Stumm, zertifizierter Auditor für ISO 27001-Audits auf der Basis von IT-Grundschutz, in Übereinstimmung mit dem Zertifizierungsschema des Bundesamtes für Sicherheit in der Informationstechnik (BSI) geprüft. Die im Auditbericht enthaltenen Schlussfolgerungen des Auditors sind im Einklang mit den erbrachten Nachweisen.

Die durch dieses Zertifikat bestätigte Anwendung von ISO 27001 auf der Basis von IT-Grundschutz (BSI-Standard 200-2: IT-Grundschutz-Methodik) umfasst die Maßnahmenziele und Maßnahmen aus Annex A von ISO/IEC 27001 und die damit verbundenen Ratschläge zur Umsetzung und Anleitungen für allgemein anerkannte Verfahren aus ISO/IEC 27002. Dieses Zertifikat ist keine generelle Empfehlung des Untersuchungsgegenstandes durch das BSI. Eine Gewährleistung für den Untersuchungsgegenstand durch das BSI ist weder enthalten noch zum Ausdruck gebracht.

Dieses Zertifikat gilt nur für den angegebenen Untersuchungsgegenstand und nur in Zusammenhang mit dem vollständigen Zertifizierungsreport.

Bonn, den 5. Juli 2023
Bundesamt für Sicherheit in der Informationstechnik
Im Auftrag

Sandro Amendola

Sandro Amendola
Direktor

* Unter der Bedingung, dass die ab 5. Juli 2023 jährlich durchzuführenden Überwachungsaudits mit positivem Ergebnis abgeschlossen werden.

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189, D-53175 Bonn · Postfach 20 03 63, D-53113 Bonn
Tel.: +49 (0)228 9582-0 · Fax: +49 (0)228 9582-5477 · Infoline: +49 (0)228 9582-111 · Internet: www.bsi.bund.de

Datenschutz Pöllinger GmbH
Datenschutz und Informationssicherheit

Prüfbericht

Flowmium GmbH
Erich-Kästner-Str. 55
63322 Rödermark

Die Prüfung des Unternehmens sowie der Software „Zeugnisgenerator“ in Bezug auf die Verarbeitung von personenbezogenen Daten im Auftrag ergibt, dass die Flowmium GmbH datenschutzrechtlich gut aufgestellt ist und im Laufe des Jahres 2021 zahlreiche datenschutzrechtliche Prozesse bezüglich der Anforderungen der EU Datenschutz-Grundverordnung (DS-GVO) weiterentwickelt und optimiert wurden.
Das Datenschutzmanagementsystem der Flowmium GmbH wurde durch ein eigeninitiativ gewünschtes Audit anhand von verschieden Checklisten, welche IT-Sicherheit, Backup und Datenschutz betreffen, durchgeführt. Hierbei wurde festgestellt, dass die Flowmium GmbH bereits sehr gut aufgestellt ist. Anhand von einer Defizitliste wurde der Flowmium GmbH eine Handlungsempfehlung übergeben, damit das Datenschutzmanagement für die Zukunft noch weiter ausgebaut und kontinuierlich optimiert werden kann.

Die Software „Zeugnisgenerator“ erfüllt die Anforderungen nach Privacy by Design und Privacy by Default nach Artikel 25 DS-GVO. Der Kunde, als verantwortliche Stelle, kann dabei entsprechende Maßnahmen treffen und ist für die Umsetzung der entsprechenden Einstellungen innerhalb der Software selbst verantwortlich.

Weiterhin werden die Grundsätze der Verarbeitung von personenbezogenen Daten, insbesondere Transparenz, Treu und Glauben, Zweckbindung und Datenminimierung entsprechend beachtet. Es werden grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet.
Der Kunde, als Verantwortlicher, hat die Rechtmäßigkeit der Datenverarbeitung selbst sicherzustellen und kann den Umfang der Verarbeitung entsprechend über die Software selbst steuern. Zudem hat der Kunde die Möglichkeit, den Zugang anhand eines Berechtigungskonzepts selbst zu steuern. Entsprechende datenschutzrechtliche Voreinstellungen sowie zusätzliche technische und organisatorische Maßnahmen stellen dabei sicher, dass Unbefugte keinen Zugriff auf die Software erhalten.

Ferner hat die Flowmium GmbH ein umfangreiches Datenschutz- und IT-Sicherheitskonzept aufgestellt und daraus entsprechende technische und organisatorische Maßnahmen abgeleitet, welchen den Anforderungen an die Sicherheit der Verarbeitung nach Art. 32 DS-GVO genügen.

Dresdner Straße 38
92318 Neumarkt
kontakt@datenschutz-poellinger.de
09181/270 577 0
www.datenschutz-poellinger.de

Zudem sind bereits in der Vergangenheit entsprechende Prozesse implementiert worden, um die kontinuierliche Verbesserung der Prozesse und Prüfung und Weiterentwicklung dieser Maßnahmen unter Berücksichtigung des Stands der Technik, der Implementierungskosten dem Umfang der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen sicherzustellen.

Die Mitarbeiter der Flowmium GmbH wurden durch eine Online-Schulung „Datenschutz und Informationssicherheit im Unternehmen“ im September 2021 geschult. Nach der Online-Schulung fand eine Prüfung zur Erlangung des Zertifikates statt. Alle Mitarbeiter haben die Prüfung mit Erfolg bestanden. Ferner wurden alle Mitarbeiter auf Datenschutz und Vertraulichkeit verpflichtet.

Zusammenfassend kann festgehalten werden, dass die Software in ihrer Konzeption und Umsetzung die Anforderungen an Entwicklung und Betrieb von Software im Sinne der EU DS-GVO umfassend erfüllt. Gleiches gilt für die Organisation und das Datenschutzmanagement in Bezug auf die Auftragsverarbeitung für die Kunden der Flowmium GmbH.

Gisela Pöllinger

Neumarkt, den 24.09.2021

Gisela Pöllinger
Auditorin für Datenschutz & Informationssicherheit

Datenschutz Pöllinger GmbH
Datenschutz und Informationssicherheit

DESAG
Sachverständiger
Gisela Pöllinger
DS/210501

Dresdner Straße 38
92318 Neumarkt
kontakt@datenschutz-poellinger.de
09181/270 577 0
www.datenschutz-poellinger.de

binsec

ZERTIFIKAT

Penetrationstest

Für die **Flowmium GmbH** aus Rödermark
führte die binsec GmbH vom
9. bis 13. Januar 2023 einen Penetrationstest durch.

Prüfgegenstand

Die Webanwendung der Flowmium GmbH zur Erstellung von Arbeitszeugnissen wurde einem Penetrationstest unterzogen. Für die Untersuchung der Webanwendung wurde eine Testumgebung zur Verfügung gestellt. Der Penetrationstest wurde als externer Grey-Box-Test durchgeführt, ohne aggressive Angriffstechniken wie DDoS-Attacken zu verwenden. Die Untersuchungsmethode orientierte sich am OWASP Testing Guide und an den OWASP TOP 10.

Prüfergebnis

Im Rahmen des Penetrationstests wurden Schwachstellen identifiziert, welche bis zum 23. Januar 2023 erfolgreich behoben wurden. Dies wurde von der binsec GmbH in einer Nachprüfung verifiziert.

Erläuterung

In einem Penetrationstest werden IT-Systeme oder IT-Anwendungen basierend auf einer strukturierten Vorgehensweise unter Verwendung von Hacking-Tools und -Techniken auf Schwachstellen hin analysiert. Die Ergebnisse des Penetrationstests sind immer eine Momentaufnahme der IT-Sicherheit. Je länger dieser zurückliegt und je mehr Änderungen vorgenommen werden, desto geringer wird die Aussagekraft der Ergebnisse. Ein Penetrationstest sollte somit jährlich oder nach signifikanten Änderungen wiederholt werden. Mehr Informationen zu den Penetrationstests der binsec GmbH finden Sie im Web unter `https://binsec.com/pentest/`.

Dominik Sauer, ppa
Head of Penetration Testing