Vertrag betreffend Auftragsdatenverarbeitung

Dieser Vertrag betreffend Auftragsdatenverarbeitung, einschliesslich seiner Anlage (Data Processing Agreement; nachfolgend "**DPA**") ist Teil der Kooperation (definiert in Präambel) zwischen dem **Auftraggeber** (definiert auf Seite 8 dieses DPA) und Okomo AG, einer Schweizerischen Aktiengesellschaft mit Sitz an der Sihleggstrasse 23, 8832 Wollerau (Schweiz) eingetragen im Schwyzer Handelsregister unter der Nr. 328.837.288 (nachfolgend "**Auftragnehmer**", "**Okomo**") für die Nutzung der Services im Rahmen der Kooperation. Auftraggeber und Auftragnehmer bilden zusammen "Parteien" und einzeln je eine "Partei".

Wie dieses DPA rechtskräftig eingegangen werden kann:

Dieses DPA wurde von Okomo vollständig und sorgfältig vorbereitet. Damit dieses DPA zwischen Auftraggeber und Aufragnehmer rechtskräftig bindend wird, muss der Auftraggeber die Informationen auf Seite 8 dieses DPA vollständig und korrekt ausfüllen und anschliessend an legal@okomo.com senden. Anschliessend erhält der Auftraggeber dieses DPA in gegengezeichneter Form vom Auftragnehmer zurück. Das Datum des Inkrafttretens ist das Datum, an dem beide Parteien dieses DPA unterzeichnet haben. Sämtliche vertragliche Anpassungen, die vom Auftraggeber an diesem DPA vorgenommen werden, sind unwirksam und nicht rechtskräftig.

Präambel

Die Parteien haben vereinbart, eine Zusammenarbeit zur Bereitstellung und Durchführung von Online-Dienstleistungen und generell damit verbundenen Dienstleistungen anzubieten. Insbesondere soll dabei die Kommunikationslösung des Auftragnehmers ("Services") zur digitalen Online-Kommunikation für Online-Dienstleistungen, virtuelle Events, andere digitale Online-Veranstaltungen oder Kommunikationsplattformen des Auftraggebers verwendet werden ("Kooperation"). Im Rahmen der Kooperation hat der Auftraggeber den Auftragnehmer beauftragt, die vom Auftraggeber an den Auftragnehmer gelieferten Personendaten zum Zweck der Durchführung der Kooperation sowie zu den Zwecken der Zurverfügungstellung der Services zu verarbeiten. Dieses DPA regelt die Rechte und Pflichten der Parteien mit Bezug auf den Datenschutz im Rahmen der Kooperation.

1. Geltungsbereich und Grundsätze

Das DPA findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter des Auftragnehmers oder durch ihn beauftragte Unterauftragnehmer (Subunternehmer) personenbezogene Daten des Auftraggebers verarbeiten.

Die Parteien verpflichten sich, die anwendbaren Datenschutzbestimmungen jederzeit einzuhalten, insb. das Bundesgesetz über den Datenschutz (DSG) und die dazugehörige Verordnung (VDSG) sowie – sofern und soweit anwendbar – auch die Vorschriften der Europäischen Datenschutzgrundverordnung (EU-DSGVO).

Die Parteien beachten im Zusammenhang mit Personendaten insbesondere die Prinzipien der Verhältnismässigkeit, der Zweckbindung, der Transparenz und von Treu und Glauben.

2. Gegenstand und Dauer der Verarbeitung

Der Auftragnehmer nimmt folgende Datenverarbeitungen vor:

- Personenbezogene Daten zur Zurverfügungstellung der Services.
- Telemetriedaten (anonymisierte Daten) Verbesserung der Services und Erstellung von Statistiken für die Auftraggeberin.

Die Verarbeitung findet im Rahmen der Kooperation statt und beruht auf diesem DPA.

Die Verarbeitung beginnt mit Start der Kooperation, welche das Datum der beidseitigen Unterzeichnung dieses DPA darstellt, und endet mit Kündigung dieses DPA oder Beendigung der Kooperation.

Die Kündigung des DPA hat schriftlich unter Einhaltung einer Kündigungsfrist von zwei (2) Wochen zu erfolgen.

3. Art und Zweck der Datenerhebung, -verarbeitung oder -nutzung

Die Verarbeitung ist folgender Art:

- Erhebung und Verarbeitung von personenbezogenen Daten im Rahmen der Zurverfügungstellung der Services für den Auftraggeber, deren Nutzung jedoch ausschliesslich durch schriftliche Aufforderung des Auftraggebers
- Erhebung, Verarbeitung und Nutzung von Telemetriedaten in anonymisierter Form im Rahmen der Verbesserung der Services und Erstellung von ergänzenden Informationen (bspw. Statistiken)

Die Verarbeitung dient folgendem Zweck:

Die Datenverarbeitung erfolgt zum Zwecke der Erbringung der vertraglichen oder vorvertraglichen Leistungen der Auftragnehmerin und Pflichten im Rahmen der Kooperation.

Es werden folgende Daten verarbeitet:

- Personenbezogene Daten von Kunden des Auftraggebers (insbesondere Name, E-Mailadresse, Chat-Verläufe, geteilte Dokumente und vereinbarte Online-Termine)
- Personenbezogene Daten von Mitarbeitenden des Auftraggebers (insbesondere Name, E-Mailadresse, Passwort (Hash), Position, Chat-Verläufe, Profilfoto, Sprache, Status, Profilbeschreibung, Filter, Kunden-Bewertungen, geteilte Dokumente, vereinbarte Online-Termine)
- Telemetriedaten in anonymisierter Form von Kunden und Mitarbeitenden des Auftraggebers (inter alia Datum und Uhrzeit, Browser, Betriebssystem, Sprache, Aktionen, Gerätetyp)

Kunden des Auftraggebers können im Rahmen ihrer Anfragen per Live-Chat und Offline-Nachricht neben den in Punkt 3 aufgeführten personenbezogenen Daten auch besonders schützenswerte Personendaten an den Auftraggeber übermitteln, welche durch den Auftragnehmer verarbeitet werden können, da sie auf einer Datenbank des Auftragnehmers gespeichert werden, wobei der Auftragnehmer ausschliesslich durch schriftliche Aufforderung des Auftraggebers auf diese besonders schützenswerte Personendaten zugreifen wird.

Von der Verarbeitung sind folgende Kategorien von Personen betroffen:

- Kunden, Interessierte und sämtliche andere Parteien, die die Online-Dienstleistung des Auftraggebers über die Services in Anspruch nehmen oder testen
- Kunden, Interessierte und sämtliche andere Parteien, die andere Online-Dienstleistungen des Auftraggebers in Anspruch nehmen, bei denen die Services eingesetzt werden, sofern die Services durch den Auftraggeber auch anderweitig eingesetzt werden
- Mitarbeitende des Auftraggebers, die die Services verwenden

4. Verschlüsselung und Löschung von Daten

Sämtliche Daten, die im Rahmen der Verwendung und Nutzung der Services ausgetauscht werden, werden verschlüsselt übertragen und gespeichert.

Sämtliche anderen Kommunikationskanäle, namentlich Audio, Video und Bildschirmübertragung, werden beidseitig per Ende-zu-Ende-Verschlüsselung übertragen und vom Auftragnehmer nicht gespeichert. Der Auftragnehmer hat zu keinem Zeitpunkt die Möglichkeit, sich auf derartige Informationen Zugriff zu verschaffen oder die Verschlüsselung anderweitig aufzuheben.

Sämtliche, in Punkt 3 aufgeführte Daten, zur Zurverfügungstellung der Services werden nach 12 Monaten nach Speicherung der Daten gelöscht.

5. Technische und organisatorische Massnahmen

Die Parteien verpflichten sich, alle zumutbaren, erforderlichen, technischen und organisatorischen Massnahmen zum Schutz der Personendaten zu ergreifen, namentlich zur Verhinderung von unbefugten Zugriffen von Dritten, Verlust, Beschädigung, Löschung oder Vernichtung der Daten.

Der Auftragnehmer wird technische und organisatorische Massnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen des anwendbaren Datenschutzgesetzes genügen und in Anlage A detailliert aufgeführt sind. Dabei beachten die Parteien, dass Kunden auch besonders schützenswerte Personendaten an den Auftraggeber übermitteln können, die durch den Auftragnehmer verarbeitet werden.

Die technischen und organisatorischen Massnahmen haben die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen. Neben der digitalisierten Informations- und Datensicherheit sind die Räumlichkeiten, in welchen die Daten verarbeitet werden, zutrittsgeschützt.

Bei der Umsetzung und Aktualisierung der technischen und organisatorischen Massnahmen (gemäss Anlage A) gewährleistet der Auftragnehmer ein dem Risiko angemessenes Mass an, insbesondere unter Berücksichtigung des aktuellen Stands der Technik, der Kosten der Umsetzung, der Art, des Umfangs, des Kontexts und der Zwecke der Verarbeitung sowie der verschiedenen Eintrittswahrscheinlichkeiten und der Schwere einer Verletzung der Rechte und Freiheiten der betroffenen Personen. Der Auftragnehmer anerkennt, dass sich der Auftraggeber auf die Fähigkeiten und Kenntnisse des Auftragnehmers verlässt, um die Angemessenheit einer Massnahme zu beurteilen, welche die personenbezogenen Daten im Rahmen dieses DPA zu schützen vermag.

Der Auftragnehmer sichert zu, dass die gemäss diesem Vertrag im Auftrag verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Ausgenommen sind technisch notwendige, temporäre Vervielfältigungen, soweit eine Beeinträchtigung des vereinbarten Datenschutzniveaus ausgeschlossen ist.

6. Auftragsverarbeitung und Beizug Dritter

Der Auftragnehmer verarbeitet Daten lediglich im Auftrag und ausschliesslich gemäss Weisung des Auftraggebers und nur so, wie der Auftraggeber die Personendaten auch selbst verarbeiten dürfte, es sei denn, der Auftragnehmer ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Sofern solche Verpflichtungen für ihn bestehen, teilt der Auftragnehmer diese dem Auftraggeber vor der Verarbeitung mit, es sei denn, die Mitteilung ist ihm gesetzlich verboten. Der Auftragnehmer verwendet darüber hinaus die ihm zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke oder Zwecke Dritter.

Änderungen der Leistungspflichten und Weisungen haben schriftlich zu erfolgen.

Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung des Auftraggebers gegen anwendbare Gesetze verstösst. Er darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und andere für den Auftragnehmer tätigen Personen untersagt ist, die Daten ausserhalb der Weisung des Auftraggebers zu verarbeiten.

Der Auftraggeber garantiert, dass der Auftragnehmer die Daten ohne Beschränkung, zur Zurverfügungstellung der Services verarbeiten darf und dass der Auftraggeber berechtigt ist, die Daten an den Auftragnehmer zu Verarbeitung weiterzugeben.

Der Auftraggeber bestätigt, dass alle notwendigen Rechtfertigungsgründe für die Datenverarbeitung (Einwilligung der Betroffenen etc.) vorliegen.

Der Beizug von Dritten als Subunternehmer für die Leistungserfüllung ist nur zulässig, wenn die andere Partei vorher schriftlich zugestimmt hat. Die Subunternehmer, welche in der auf okomo.com/datenschutzerklaerung/ aufrufbaren Datenschutzerklärung des Auftragnehmers erwähnt sind, gelten hiermit als vom Auftraggeber explizit akzeptiert.

Zur Leistungserbringung beigezogene Dritter unterliegen denselben Pflichten wie die Parteien. Der Auftraggeber sowie der Auftragnehmer garantieren ihre Pflichten allfälligen Dritten zu überbinden. Sie bleiben für die Einhaltung der Pflichten verantwortlich.

Im Zusammenhang mit der beauftragten Verarbeitung hat der Auftragnehmer den Auftraggeber bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten sowie bei Durchführung der Datenschutzfolgeabschätzung gemäss EU-DSGVO zu unterstützen. Alle erforderlichen Angaben und Dokumentationen sind dem Auftraggeber auf Anforderung unverzüglich vorzulegen.

Wird der Auftraggeber durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich der Auftragnehmer den Auftraggeber im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.

Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Zustimmung durch den Auftraggeber erteilen. Direkt an den Auftragnehmer gerichtete Anfragen von Dritten oder Betroffenen wird er unverzüglich an den Auftraggeber weiterleiten.

Die Auftragsverarbeitung erfolgt grundsätzlich innerhalb der Schweiz und der EU. Jegliche Verlagerung in ein Drittland darf nur mit vorheriger Zustimmung des Auftraggebers und unter den in Art. 6 DSG bzw. Kapitel V EU-DSGVO enthaltenen Bedingungen sowie unter Einhaltung der Bestimmungen dieses DPA erfolgen. Eine Verarbeitung in Indien, Russland oder China ist unter keinen Umständen erlaubt.

7. Betroffenenrechte

Die Parteien verpflichten sich die Betroffenenrechte zu wahren und zu garantieren.

Die betroffene Person hat namentlich das Recht auf Auskunft, Löschung, Korrektur, Sperrung sowie – im Fall der Anwendbarkeit der EU-DSGVO – der Portabilität der Daten (Art. 12 ff EU-DSGVO / GDPR).

Können Daten aus gesetzlichen oder geschäftlichen Pflichten nicht gelöscht werden, werden sie blockiert.

Die Parteien verpflichten sich die Daten, welche die betroffene Person zur Verarbeitung zur Verfügung gestellt hat, in einem gängigen, maschinenlesebaren Format auf Anfrage der betroffenen Person herauszugeben.

Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung

oder Auskunft an den Auftragnehmer, leitet dieser die betroffene Person an den Auftraggeber weiter. Die Parteien unterstützen einander soweit vereinbart bei der Verarbeitung der betroffenen Anfragen. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

8. Dokumentation der Prozesse

Die Parteien führen Protokolle über die Verarbeitungsprozesse und dokumentieren die Datenverarbeitung.

Auf Anfrage der betroffenen Person oder der Aufsichtsstellen haben die Parteien über die Datenverarbeitung dokumentiert zu informieren.

9. Datenschutzbeauftragte Person

Die Parteien nennen einander gegenseitig einen Ansprechpartner für im Rahmen des Vertrags anfallende Fragen des Datenschutzes und falls gesetzlich vorgesehen, einen internen Datenschutzbeauftragten.

10. Mitteilungspflichten und Kontrollrechte

Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes von Personendaten bekannt werden. Sofern und soweit die EU-DSGVO anwendbar ist, melden die Parteien eine entsprechende Verletzung innert 72 Stunden auch der zuständigen Aufsichtsbehörde.

Der Auftraggeber hat das Recht - auf eigene Kosten - beim Auftragnehmer selber oder durch eine unabhängige, eingesetzte Revisionsgesellschaft Kontrollen durchzuführen bzw. durchzuführen lassen (Audit). Solche Kontrollen haben ohne vermeidbare Störungen des Geschäftsbetriebes des Auftragnehmers zu erfolgen. Soweit nicht aus vom Auftraggeber zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten des Auftragnehmers sowie nicht häufiger als alle 12 Monate statt.

11. Löschung der Daten und Rückgabe

Nach Erfüllung des Zwecks, jedenfalls aber nach Beendigung der Kooperation bzw. Ablauf oder Kündigung des DPA hat der Auftragnehmer alle Personendaten an den Auftraggeber herauszugeben oder zu löschen, es sei denn, die Parteien vereinbaren dies explizit anders. Der Auftraggeber entscheidet über die Herausgabe oder Löschung. Allfällige Kopien, die der Auftragnehmer erstellt hat, sind ebenfalls zu löschen. Auf Verlangen des Auftraggebers hat der Auftragnehmer die vollständige Herausgabe der Daten bzw. Löschung schriftlich zu bestätigen.

12. Sonderkündigungsrecht

Beide Parteien können dieses DPA jederzeit ohne Einhaltung einer Frist kündigen („**ausserordentliche Kündigung**"), wenn ein schwerwiegender Verstoss der anderen Partei gegen anwendbare Datenschutzvorschriften oder eine Bestimmung dieses DPA vorliegt.

Bei unerheblichen Verstössen gegen Datenschutzvorschriften oder eine Bestimmung dieses DPA setzt die andere Partei eine angemessene Frist zur Abhilfe. Erfolgt die Abhilfe nicht rechtzeitig, so ist die andere Partei zur ausserordentlichen Kündigung wie im vorstehenden Abschnitt beschrieben berechtigt.

13. Schriftform

Änderungen dieses DPA bedürfen der Schriftlichkeit. Selbiges gilt für die Änderung der Schriftformklausel.

14. Anwendbares Recht und Gerichtsstand

Auf dieses DPA ist ausschliesslich materielles Schweizer Recht anwendbar, unter Ausschluss des Internationalen Privatrechts (IPRG). Ausschliesslicher Gerichtsstand für Streitigkeiten aus diesem Vertrag ist Zürich, Schweiz.

[*Unterschriften auf der folgenden Seite*]

Für den Auftragnehmer:

Autorisierte Person:_____

Position:_____

Ort, Datum: _____

Für den Auftraggeber:

Firmenname:_____

Firmenadresse:_____

Autorisierte Person:_____

Position:_____

Ort, Datum: _____

ANLAGE A: TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

1. Vertraulichkeit

- **Zugangskontrolle:**
  - Zugang hat die Geschäftsführung des Auftragnehmers sowie der Senior Development Lead (alle anderen Okomo-Mitarbeitenden sind im Allgemeinen ausgeschlossen)
  - Im Rahmen von Support-Leistungen und anderen unterstützenden Massnahmen zum Zweck der Durchführung der Kooperation sowie zu den Zwecken der Zurverfügungstellung der Services können ausnahmsweise auch andere Mitarbeitende des Auftragsnehmer Zugang erhalten
  - Zugang ist geschützt durch Microsoft Azure-Active Directory (inkl. essentielle Voraussetzungen: sicheres Passwort und Zwei-Faktor-Authentifizierung)
  - Generell absolvieren alle Mitarbeitenden des Auftragnehmers bei Eintritt ins Unternehmen eine umfassende Schulung zu den Themen Datenschutz und Datenumgang und unterzeichnen zudem eine Geheimhaltungsvereinbarung, die sie insbesondere dazu verpflichtet, gemäss den entsprechenden Datenschutzbestimmungen zu agieren

- **Zugriffskontrolle:**
  - Zugriff möglich über Microsoft Azure-Portal für in Punkt 1 genannte Personen
  - Zugriffe auf Datenbanken und Datenspeicher werden geloggt (=aufgezeichnet)
  - Kontrolle und Überwachung von Logdaten werden monatlich durchgeführt

- **Trennungskontrolle:**
  - Innerhalb der Services werden Administratoren und Experten eindeutig mittels der Authentifizierung (=Login) identifiziert
  - Eine Interaktion wird jeweils einem Experten und einem Endkunden mittels Interaktions-ID zugewiesen
  - Der Endkunde wird über diese Interaktions-ID identifiziert
  - Chat-Inhalte (Live-Chat) und Dokumente können dadurch jederzeit eindeutig einem Experten und einem Endkunden zugewiesen werden
  - Die Kanäle Audio-Chat, Video-Chat und Screen-Sharing werden direkt zwischen Experten und Endkunden mittels Peer-to-Peer-Verbindung aufgebaut und sind Ende-zu-Ende Verschlüsselt (Secure Real-time Transport Protocol, SRTP). Dadurch können sie weder aufgezeichnet, abgespeichert noch von dem Auftragnehmer, Siemens oder einer anderen Drittpartei (ausser dem jeweiligen Experten und Endkunden) eingesehen werden

- **Pseudonymisierung:**
  - Der Auftragnehmer speichert anonymisierte Telemetriedaten zur Nutzung und Verbesserung der Services und zur Statistikerhebung. Diese Telemetriedaten beinhalten keine IP-Adressen und erlauben keinen Rückschluss auf einzelne Personen.

- **Verschlüsselung:**
  - Sämtliche übertragenen Daten werden verschlüsselt ausgetauscht (HTTPS)
  - Sämtliche erhobenen Daten werden verschlüsselt abgespeichert
  - Audio-Chat, Video-Chat und Screen-Sharing werden mittels Ende-zu-Ende-Verschlüsselung zwischen Experten und Endkunden verschlüsselt

- **Datensicherung/Backup:**
  - Alle 4 Stunden wird ein volles Datenbank-Backup erzeugt und auf einer separaten Serverinstanz verschlüsselt abgespeichert. Die Backups werden regelmässig geprüft und eine Wiederherstellung der Datenbank wurde trainiert. Backups werden nach 30 Tagen gelöscht.

2. Integrität

- **Weitergabekontrolle:**
  - Zugriffskontrolle wie in Punkt 1 beschrieben
  - Verschlüsselung wie in Punkt 1 beschrieben
  - Geräte der Okomo-Mitarbeiter: Firewall und Virenschutz

- **Eingabe-/Verarbeitungskontrolle:**
  - Protokollierung und Auswertung der Änderung an Daten, Anwendungen und Systemen
  - Protokollierung und Auswertung der Administrator-Aktivitäten

3. Verfügbarkeit und Belastbarkeit

- **Verfügbarkeitskontrolle:**
  - Datensicherung/Backup wie in Punkt 1 beschrieben
  - Die Services laufen auf diversen Hosted-Diensten auf Microsoft Azure im Hochsicherheits-Rechenzentrum mit einer durchschnittlichen Verfügbarkeit von 99.95%
  - Die effektive Verfügbarkeit der Services wird mittels Monitoring-Service laufend geprüft, und über Ausfälle wird der Auftragnehmer laufend via Live-Benachrichtigung automatisch informiert.

- **Wiederherstellung:**
  - Bei einem Service-Ausfall kann der Auftragnehmer allfällige Probleme (die nicht einem Fehler der Microsoft Azure-Dienste zuzuschreiben sind) basierend auf Infrastruktur-Log-Daten systematisch und effizient lösen. Können Probleme nicht innerhalb der ersten halben Stunde gelöst werden, wird zusätzlich ein Support-Ticket bei Microsoft Azure-Support erstellt, welcher sich im Regelfall innerhalb einer Stunde meldet.
  - Datensicherung/Backup wie in Punkt 1 beschrieben

4. Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Massnahmen

- **Datenschutz-Management:**
  - Siehe Ausführungen Punkt 1

- **Incident-Response-Management:**
  - Siehe Beschreibung Punkt 1 zu Verfügbarkeitskontrolle und Wiederherstellung

- **Datenschutzfreundliche Voreinstellungen:**
  - Siehe Ausführungen Punkt 1

- **Auftragskontrolle:**
  - Siehe Ausführungen Punkt 1

- **Risikomanagement:**
  - Datensicherung/Backup wie in Punkt 1 beschrieben
  - Die Services laufen auf Microsoft Azure-Diensten, die laufend aktiv vom Zulieferer weiterentwickelt werden. Das heisst, Sicherheitspatches werden in regelmässigen monatlichen Abständen von dem Auftragnehmer eingespielt und geprüft.
  - Der Auftragnehmer prüft in regelmässig wöchentlichen Abständen die eingesetzten Entwicklungs-Libraries auf bekannte Schwachstellen und kann dadurch aktiv auf neue Schwachstellen agieren. Daneben werden Library-Abhängigkeiten so aktuell wie möglich gehalten.
  - In der Okomo-Plattform ist CORS (Cross-Origin Resource Sharing) und CSP (Content Security Policy) sind aktiviert und verhindern Cross-Site Request Forgery, Cross-Site-Scripting (XSS), Clickjacking, Code Injection Attacks).
  - Passwörter von Administratoren und Experten werden nicht im Plaintext-Format abgespeichert, sondern als Hash (BCrypt)
  - Die Geräte der Okomo-Mitarbeiter und -Geschäftsführung werden regelmässig gewartet (Updates), ein Antiviren-Programm ist aktiv, und die Geräteverschlüsselung ist aktiv.