

Handreichung für Datenschutzbeauftragte

XLeap ist eine Lösung zur Vorbereitung und zum Treffen von Entscheidungen und für die kreative Lösung von Problemen. Hierfür bietet XLeap eine Reihe virtueller Arbeitsbereiche, in denen Teilnehmer Fakten, Meinungen und Ideen brainstormen, durchdringen und priorisieren können. Per Vorgabe sind Beiträge vollständig anonym. Es gibt keine Verknüpfung zwischen beitragender Person und Beitrag, auch nicht auf technischer Ebene.

XLeap ist nach dem Grundsatz der Datensparsamkeit entwickelt. Benutzerkonten werden ausschließlich zur Lizenzierung und Authentifizierung eingerichtet. Nicht mehr benötigte Sessions und inaktive Benutzer werden automatisch gelöscht. Aktivitäts- oder personenbezogene Auswertungen werden nicht unterstützt. Sämtliche Daten eines XLeap Centers sind Eigentum des Kunden und werden durch seine Administratoren gesteuert. MeetingSphere GmbH, das Unternehmen, das XLeap entwickelt und bereitstellt, nutzt Kundendaten nicht für eigene Zwecke und teilt diese mit niemandem.

Paragraph 11 der [Terms and Conditions for the Software Service – International](#)^(1) 2) lautet:

11. Datenschutz

11.1 Umfang. Sie erkennen an, dass Sie die Anwendungsdienstleistung in einem Modell geteilter Verantwortung nutzen. Dieser Paragraph 11 definiert die Verantwortlichkeiten und Zusicherungen zwischen Ihnen und dem Provider in Sachen Datenschutz unter besonderer Berücksichtigung der EU-Datenschutzgrundverordnung (DSGVO) und erweitert die Geschäftsbedingungen zum Vertrag über die Auftragsdatenverarbeitung im Sinne der DSGVO.

11.2 Rollen. Im Zusammenhang dieser Vereinbarung handelt der Provider als Auftragsverarbeiter. Sie agieren als Verantwortlicher und können dabei ebenfalls Auftragsverarbeiter im Sinne der DSGVO sein.

11.3 Arten gesammelter Information. Der Anwendungsdienst sammelt ein Minimum personenbezogener Daten über die Nutzer des Dienstes, die Beiträge dieser Nutzer sowie situationsbezogene Daten wie folgt:

11.3.1 Personenbezogene Daten. Der Anwendungsdienst sammelt personenbezogene Daten ausschließlich zum Zweck der Authentifizierung der Benutzer bei Anmeldung sowie der Identifizierung der Benutzer in Sessions. Die erhobenen Daten sind beschränkt auf (a) Vorname und Nachname, (b) Emailadresse und (c) Organisation bzw. Abteilung.

11.3.2 Beiträge von Benutzern. Benutzer und ihre Beiträge fallen in zwei Kategorien: (a) Teilnehmer, die Ideen, Kommentare und Bewertungen beitragen, welche Datei-Anhänge enthalten können und (b) Moderatoren, die Sessions mit Teilnehmern aufsetzen und dabei Strukturen beitragen wie Agenden und Fragen, mit denen Sie die Teilnehmer in ihrer Arbeit anleiten.

11.3.3 Situative Daten. Diese sind Informationen, die zum Zweck von Sicherheitsüberprüfungen erhoben werden. Dazu gehören IP-Adressen, von denen sich Benutzer verbinden und die Erzeugung, der Abruf und die Veränderung von Datensätzen. Der Provider sichtet und analysiert diese Logs ausschließlich zur Sicherung des Betriebs und zum Schutz der im System gesammelten Informationen. Der Provider löscht Auditlogs nach 90 Tagen.

11.4 Pflichten und Verantwortlichkeiten des Providers. Der Provider implementiert und unterhält organisatorische und technische Vorkehrungen, um Ihre Daten angemessen und in Übereinstimmung mit den Anforderungen der DSGVO und dem Prinzip der Datengeheimhaltung zu schützen.

11.4.1 Verarbeitung. Der Anwendungsdienst verarbeitet personenbezogene Daten und Beiträge von Benutzern nur insofern, als er die technische Funktionalität bereitstellt, mit der Ihre Benutzer solche Informationen eingeben, ändern oder löschen. Zur Klarstellung: Der Provider verarbeitet personenbezogene Daten ausschließlich durch (a) Bereitstellung der technischen Funktionen, die Sie im Rahmen der Anwendungsdienstleistung nutzen um personenbezogene Daten zu verarbeiten, (b) Erstellung, Wiederherstellung und Löschung von Sicherungskopien Ihrer Center-Datenbank, die solche Informationen enthält, (c) Erstellung, Speicherung und Löschung von Audit-Logs und (d) Speicherung von Lizenzinformationen im Subskriptions-Store.

11.4.2 Speicherung. Durch den Anwendungsdienst gesammelte Informationen werden in verschlüsselter Form ausschließlich am vereinbarten Ort gespeichert, von wo sie in verschlüsselter Form direkt an Benutzer übertragen werden. Zur Klarstellung: Der Provider wird Ihre personenbezogenen oder sonstigen Daten nicht außerhalb des

vereinbarten Ortes speichern. Er hostet die Center von Gebietsansässigen der Europäischen Union in der Europäischen Union. Sie können den Provider anweisen, Ihr Center in London oder Singapur oder einer anderen einvernehmlich bestimmten AWS-Region zu hosten.

11.4.3 Weitergabe gesammelter Informationen. Der Provider wird durch den Anwendungsdienst gesammelte Informationen niemandem bekanntmachen oder weitergeben, es sei denn, eine Herausgabe ist gesetzlich vorgeschrieben.

11.4.4 Unterverarbeitung. Die Anwendungsdienstleistung basiert auf den Infrastrukturdienstleistungen von Amazon (AWS) in der Verantwortung des Providers. Die Vereinbarung zwischen dem Provider und AWS erfüllt die Anforderungen der DSGVO an einen Vertrag zur Auftragsverarbeitung. Der Provider wird Sie über jede Veränderung bezüglich der Unterverarbeitung unterrichten.

11.4.5 Personal. Der Provider gewährleistet, dass alle mit der Verarbeitung Ihrer Daten befassten Personen hinsichtlich ihrer polizeilichen Führung überprüft, bezüglich der Anforderungen der DSGVO und der Datengeheimhaltung geschult und auf deren Einhaltung verpflichtet wurden.

11.4.6 Verschlüsselung. Der Provider garantiert, dass Informationen nur verschlüsselt gespeichert und an Benutzer übertragen werden.

11.4.7 Nutzung durch den Provider. Der Provider nutzt durch die Anwendungsdienstleistung gesammelte Informationen nicht. Zur Klarstellung: Der Provider nimmt kein ‚Profiling‘ von Nutzungsmustern, Benutzerbeiträgen, personenbezogenen Daten oder anderweitig verknüpften Informationen vor, und zwar weder für bestimmte noch unbestimmte Zwecke, und wird Dritte an einer solchen Nutzung hindern.

11.4.8 Andere Systeme. Die durch Ihre Nutzung des Anwendungsdiensts gesammelten Informationen werden gespeichert in (a) einer gesonderten Center-Instanz mit gesonderter Datenbank, (b) Sicherungskopien dieser Datenbank und (c) dem Subskriptions-Store. Der Subskriptions-Store befindet sich in Dublin (Europäische Union) und speichert ausschließlich die Namen und Emailadressen Lizenzierter Benutzer, Subskriptionsadministratoren und Lizenzierer. Der Provider bewahrt diese lizenzrelevanten Informationen im Rahmen der gesetzlichen Bestimmungen und nach den Regeln ordnungsgemäßer Geschäftsführung als Teil seiner Geschäftsunterlagen auf.

11.4.9 Löschung. Der Provider löscht ihr Center samt Datenbank und Sicherungskopien am Ende der dreimonatigen Nachfrist oder auf Ihre schriftliche Anweisung. Auf Ihren schriftlichen Auftrag löscht der Provider Sicherungskopien Ihres Centers, sollte dieses erforderlich sein, damit Sie einer Löschanweisung vollumfänglich nachkommen können. Zur Klarstellung: Nach einer solchen Löschung sind keine weiteren Kopien Ihrer Daten vorhanden und Sie erkennen an, dass solche Daten auch nicht wiederhergestellt werden können.

11.4.10 Nutzungsstatistiken. Zur Verbesserung des Produkts führt der Provider anonymisierte Nutzungsstatistiken für Systemkomponenten. Die Statistik kann nicht auf einzelne Benutzer oder Benutzergruppen heruntergebrochen werden.

11.4.11 Benachrichtigung bei Datenschutzverletzungen. Der Provider wird Sie bei materiellen Verstößen durch den Provider, sein Personal oder durch Dritte gegen Vorschriften zum Schutz Ihrer personenbezogenen Daten oder gegen die in diesem Vertrag getroffenen Festlegungen unverzüglich unterrichten. Der Provider trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die Betroffenen und spricht sich hierzu unverzüglich mit Ihnen ab. Der Provider wird Sie bei der Erfüllung Ihrer Informationspflichten gegenüber den Datensubjekten unterstützen.

11.4.12 Anfragen Betroffener. Auf Ihre schriftliche Anforderung wird der Provider Sie dabei unterstützen, Betroffenen Auskünfte zur Erhebung, Verarbeitung oder Nutzung ihrer Daten Rahmen Ihrer Nutzung der Anwendungsdienstleistung zu erteilen. Sie und der Provider erkennen das Recht von Personen, die unter den Schutz der DSGVO fallen, an, Auskunft zu ihren Daten nach den Bestimmungen der DSGVO zu erhalten, und werden diesen Personen angemessenen Zugang zu ihren Daten zu ermöglichen. Sie und der Provider werden zudem angemessene Maßnahmen treffen, um betroffenen Personen die Korrektur, Ergänzung oder Löschung solcher personenbezogenen Daten zu ermöglichen, die nachweislich falsch oder unvollständig sind. Individuen können den Zugang zu ihren Daten bzw. die Löschung, Korrektur oder Ergänzung dieser Daten gemäß den Bestimmungen der DSGVO beantragen unter privacy@meetingsphere.com.

11.5 Ihre Pflichten. Während der Provider für die technische Sicherheit, Verfügbarkeit, Vertraulichkeit und Funktionalität der Anwendungsdienstleistung verantwortlich ist, obliegt es Ihnen, die Nutzung der Anwendungsdienstleistung in Übereinstimmung mit der DSGVO, den Prinzipien der Datensicherheit und anderen Sie betreffenden Bestimmungen zu gewährleisten. Diese Verpflichtung beinhaltet die nachfolgenden Unterabschnitte dieses Paragraphen 11.5, ist jedoch nicht auf diese beschränkt:

11.5.1 Sammlung Personenbezogener Daten. Sie werden personenbezogene Daten nur mit Zustimmung des jeweiligen Benutzers erheben und/oder wo Sie ein legitimes Interesse oder rechtlich Grundlage dafür haben.

11.5.2 Authentifizierung. Sie werden zum Schutz personenbezogener Daten Ihrer Benutzer angemessene Authentifizierungsanforderungen sowie eine Trennung von Rollen festlegen und durchsetzen.

11.5.3 Datensparsamkeit. Sie erkennen an, dass der Anwendungsdienst kein Aufbewahrungsmedium für die Ergebnisse und Protokolle von Sessions ist. Sie werden Ihre Administratoren und Moderatoren anweisen, personenbezogene Daten zu löschen, wenn diese ihren Zweck erfüllt haben, und die automatisierten Routinen des Anwendungsdienstes im Sinne der Datengeheimhaltung und -Sparsamkeit einzusetzen zur Löschung inaktiver Benutzerkonten sowie alter, ungenutzter Sessions, die Teilnehmerlisten enthalten können.

11.5.4 Unregelmäßigkeiten. Sie werden Ihre Administratoren belehren, dass jeder Versuch, die Schutzmechanismen der Anwendungsdienstleistung gegen den Export, das ‚Profiling‘ oder die Übertragung personenbezogener Daten zu umgehen oder auszuhebeln, ein schwerwiegender Verstoß gegen diesen Vertrag und möglicherweise strafbar sind.

Begriffsdefinitionen (Auszug)

“Center” meint die technische Umgebung, in der Sessions geplant, durchgeführt und aufbewahrt werden.

“DSGVO” bezeichnet die auch als ‘GDPR’ bekannte Datenschutzgrundverordnung der Europäischen Union.

“MeetingSphere” bezeichnet MeetingSphere GmbH eine in Hamburg HRB 153862 eingetragene Gesellschaft beschränkter Haftung, Efftingestrasse 28, 22041 Hamburg, die in diesem Vertrag durchgängig als ‚Provider‘ bezeichnet wird.

“Moderator” meint eine benannte Person, die von einem Subskriptionsadministrator oder Lizenzierer durch eine Benutzersubskription lizenziert wurde, Sessions durchzuführen.

“Nachfrist” ist der in Wochen oder Monaten bemessene Zeitraum, für den ein Center nach Ablauf der Center Subskription erhalten bleibt zwecks nachträglicher Verlängerung.

“Personenbezogene Daten” sind 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 identifiziert werden kann.

“Session” bezeichnet Konferenzen, Meetings, Sitzungen und Workshops in denen Teilnehmer die Anwendungsdienstleistung nutzen, um miteinander zu kommunizieren oder um die Ergebnisse ihrer Arbeit zu dokumentieren oder mitzuteilen. Solche Konferenzen, Meetings, Sitzungen und Workshops können an einem Ort stattfinden oder über ein Netzwerk gleichzeitig oder zeitversetzt. Sie müssen durch einen authentifizierten Moderator gesteuert sein.

“Subskriptions-Store” bezeichnet das System des Providers zur Verwaltung von Subskriptionen und zur Bereitstellung der Anwendungsdienstleistung.

1) *Inoffizielle Übersetzung. Es gilt der Text des englischsprachigen Originals.*

2) Die ‚[Terms and Conditions for the Software Service – International](#)‘ gelten für ‚XLeap Center‘ und ‚Managed Server‘. Die ‚[Terms and Conditions for Personal Subscriptions – International](#)‘ unterscheiden sich bezüglich der Details der technischen Implementierung.