AUFTRAGSVERARBEITUNGSVERTRAG

Zuletzt aktualisiert am 14. August 2026

Dieser **AUFTRAGSVERARBEITUNGSVERTRAG** (nachfolgend auch „**Vertrag**“) ist ein rechtsverbindlicher Vertrag zwischen AJAX SYSTEMS TRADING FZE (nachfolgend „**Ajax**“ oder „**Auftragsverarbeiter**“) und dem Verantwortlichen für Produkte und Software von Ajax, wie im Abschnitt 1 dieses Vertrags definiert (nachfolgend auch „**Verantwortlicher**“), einzeln als „Partei“ und gemeinsam als die „Parteien“ bezeichnet.

Durch die Nutzung der Produkte und -Software von Ajax akzeptiert der Endnutzer diesen Vertrag und geht diesen ein; der Endnutzer (und, falls zutreffend, sein Unterzeichner) sichert zu und gewährleistet, dass der Endnutzer und sein Unterzeichner über die Rechtsfähigkeit und Befugnis verfügen, diesen verbindlichen Vertrag einzugehen und dessen Bestimmungen einzuhalten, und dass der Endnutzer in Übereinstimmung mit diesem Vertrag und allen geltenden Gesetzen handeln wird.

HINTERGRUND UND ZWECK

A. Im Rahmen dieses Vertrags sind der Auftragsverarbeiter, der Verantwortliche und alle relevanten Dritten (d. h. Unterauftragsverarbeiter), die im Vertrag angegeben und von beiden Parteien genehmigt wurden, an der Erbringung der Dienstleistungen beteiligt, was die Verarbeitung personenbezogener Daten (wie unten definiert) durch den Auftragsverarbeiter im Auftrag des Verantwortlichen erfordert. Der Auftragsverarbeiter kann personenbezogene Daten im Auftrag des Verantwortlichen gemäß den Bestimmungen dieses Vertrags und all seiner wesentlichen Bestandteile, z. B. Anhänge, Änderungen usw., verarbeiten.

B. Die Parteien streben an, diesen Vertrag in Übereinstimmung mit den Anforderungen des geltenden Rechtsrahmens für die Datenverarbeitung sowie der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (nachfolgend auch „Datenschutz-Grundverordnung“ oder „DSGVO“) umzusetzen.

C. Zweck dieses Vertrags ist es, die Datenschutz- und Datenverarbeitungspraktiken zu vereinbaren, die bei der Erbringung der Dienstleistungen (wie unten definiert) anzuwenden sind. Dieser Vertrag und sonstige damit zusammenhängende Vertragsunterlagen stellen einen Auftragsverarbeitungsvertrag gemäß Artikel 28 der DSGVO dar. Die Parteien beabsichtigen, dass dieser Vertrag in einer Weise ausgelegt wird, die mit diesem Ziel und ihren Verpflichtungen aus der DSGVO und anderen geltenden Datenschutzgesetzen in Einklang steht. Sofern der Kontext nichts anderes erfordert, haben die in diesem Vertrag und den dazugehörigen Anlagen verwendeten Begriffe dieselbe Bedeutung wie in der DSGVO.

1. BEGRIFFSBESTIMMUNGEN UND AUSLEGUNG

Sofern in diesem Vertrag nicht anders definiert, haben die hierin verwendeten großgeschriebenen Begriffe und Ausdrücke die folgende Bedeutung:

1.1 Der Begriff „**Vertrag**“ bezeichnet diesen Auftragsverarbeitungsvertrag sowie alle Anhänge, Anlagen und ergänzenden Dokumentationen. Verweise in diesem Vertrag auf die „Endanwendervereinbarung“ beziehen sich auf die Endanwendervereinbarung von Ajax unter https://ajax.systems/end-user-agreement/;

1.2 Der Begriff „**Verantwortlicher**“ bezeichnet den Kontoinhaber, der ein Konto registriert hat, um die Produkte und Software von Ajax als Endnutzer zu verwenden, und der über die Zwecke und Mittel der

Verarbeitung personenbezogener Daten entscheidet, die vom Auftragsverarbeiter in seinem Auftrag durchgeführt wird. Der Verantwortliche kann eine natürliche oder eine juristische Person sein;

1.3 Der Begriff „**Datenschutzbestimmungen**“ bezeichnet das EU-Datenschutzrecht (einschließlich, aber nicht beschränkt auf die EU-Datenschutz-Grundverordnung 2016/679 und Gesetze zur Umsetzung oder Ergänzung der DSGVO) sowie, soweit anwendbar, die Datenschutz- oder Privatsphärengesetze jedes anderen Landes, das für die Verarbeitung im Rahmen dieses Vertrags relevant ist;

1.4 Der Begriff „**EWR**“ bezeichnet den Europäischen Wirtschaftsraum;

1.5 Der Begriff „**Personenbezogene Daten**“ bezeichnet alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, die der Auftragsverarbeiter im Auftrag des Verantwortlichen gemäß oder im Zusammenhang mit der Endanwendervereinbarung unter https://ajax.systems/end-user-agreement/ oder einer sonstigen Vereinbarung, sofern zusätzlich zwischen den Parteien vereinbart, verarbeitet.

1.6 Der Begriff „**Dienstleistungen**“ bezeichnet die vom Auftragsverarbeiter für den Verantwortlichen im Zusammenhang mit den Produkten und Software von Ajax erbrachten Dienstleistungen.

1.7 Der Begriff „**Anweisungen**“ bezeichnet jede vom Verantwortlichen an den Auftragsverarbeiter erteilte Anweisung bezüglich der Verarbeitung personenbezogener Daten, unabhängig davon, ob diese (a) über die Funktionalität der Produkte und Software von Ajax; (b) durch technische Vereinbarungen, Anhänge oder sonstige mit dem Auftragsverarbeiter vereinbarte Dokumentationen; oder (c) auf sonstige Weise schriftlich zwischen den Parteien vereinbart erteilt wird. Zur Vermeidung von Zweifeln ist der Auftragsverarbeiter nicht verpflichtet, die Rechtsgrundlage oder Angemessenheit von Anweisungen zu prüfen, es sei denn, diese stehen im Widerspruch zu den geltenden Datenschutzbestimmungen.

1.8 Der Begriff „**Unterauftragsverarbeiter**“ bezeichnet jeden relevanten Dritten, der vom oder im Namen des Auftragsverarbeiters beauftragt wird, personenbezogene Daten und sonstige damit zusammenhängende Daten im Auftrag des Verantwortlichen gemäß den Bestimmungen dieses Vertrags zu verarbeiten.

1.9 Der Begriff **„Produkte und Software von Ajax“** bezeichnet die Hardware-Produkte und dazugehörige Software, die von Ajax im Rahmen der Endanwendervereinbarung unter https://ajax.systems/end-user-agreement/ zur Verfügung gestellt werden.

2. ZWECKE DER DATENVERARBEITUNG

2.1 Gegenstand der Verarbeitung im Rahmen dieses Vertrags sind die personenbezogenen Daten, die durch oder im Zusammenhang mit der Nutzung der Produkte und Software von Ajax durch den Verantwortlichen erzeugt werden und die der Auftragsverarbeiter im Auftrag des Verantwortlichen zu den in diesem Abschnitt 2 genannten Zwecken verarbeitet.

2.2 Die Verarbeitung umfasst das Erheben, das Speichern, die Organisation, die Übermittlung, das Auslesen und das Löschen von personenbezogenen Daten mittels der Cloud-Infrastruktur des Auftragsverarbeiters sowie jede sonstige Operation, die erforderlich ist, um den in Klausel 2.3 dieses Vertrags genannten Zwecken Wirkung zu verleihen.

2.3 Der Auftragsverarbeiter verarbeitet personenbezogene Daten gemäß den dokumentierten Anweisungen des Verantwortlichen, wie in Klausel 3.1 dieses Vertrags festgelegt, zu den folgenden Zwecken:

(a) Betreiben der Cloud-Infrastruktur, die von den Produkten und Software von Ajax erzeugte Ereignisse, Warnmeldungen und sonstige Daten empfängt, verarbeitet und speichert, sowie Übermitteln entsprechender Benachrichtigungen an den Verantwortlichen;

(b) Ermöglichen des Fernzugriffs und der Fernsteuerung der Produkte und Software von Ajax durch den Verantwortlichen, einschließlich des Zugriffs auf Aufzeichnungen und die von den Geräten erzeugte Ereignishistorie;

(c) Bereitstellen von technischem Support für den Verantwortlichen im Zusammenhang mit dessen

Nutzung der Produkte und Software von Ajax;
(d) Ermöglichen für den Verantwortlichen, durch dokumentierte Anweisungen den Zugriff auf die Produkte und Software von Ajax sowie damit zusammenhängende personenbezogene Daten mit vom Verantwortlichen autorisierten Dritten zu teilen, wie in Klausel 3.3 dieses Vertrags näher beschrieben.

2.4 Der Auftragsverarbeiter verarbeitet personenbezogene Daten für die in Abschnitt 9 dieses Vertrags festgelegte Dauer.

2.5 Die Kategorien betroffener Personen und die Kategorien personenbezogener Daten, die im Rahmen dieses Vertrags verarbeitet werden, sind in Anhang 1 aufgeführt.

3. ALLGEMEINE VERPFLICHTUNGEN BEZÜGLICH DER DATENVERARBEITUNG

3.1 **Anweisungen**. Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich:

(a) zu den in Abschnitt 2 dieses Vertrags festgelegten Zwecken;
(b) auf dokumentierte Anweisungen des Verantwortlichen; und
(c) in Übereinstimmung mit den geltenden Datenschutzbestimmungen.

Der Verantwortliche darf den Auftragsverarbeiter nicht anweisen, personenbezogene Daten unter Verletzung geltenden Rechts zu verarbeiten. Der Auftragsverarbeiter übernimmt keine Haftung für Schäden oder Nachteile, die aus der Befolgung von Anweisungen resultieren, zu deren Erteilung der Verantwortliche rechtlich nicht berechtigt war. Ist der Auftragsverarbeiter begründeter Ansicht, dass eine Anweisung gegen geltende Datenschutzbestimmungen verstößt, informiert er den Verantwortlichen – sofern nicht gesetzlich verboten – unverzüglich schriftlich und kann die Verarbeitung der betroffenen personenbezogenen Daten (mit Ausnahme der bloßen Speicherung und der Aufrechterhaltung der Sicherheit dieser Daten) aussetzen, bis der Verantwortliche neue Anweisungen erteilt, die der Auftragsverarbeiter befolgen kann. Während einer solchen Aussetzung haftet der Auftragsverarbeiter nicht für die Nichterfüllung von Pflichten, die von der ausgesetzten Verarbeitung abhängen.

3.2 Der Auftragsverarbeiter hält die geltenden Datenschutzbestimmungen ein und richtet angemessene Systeme und Verfahren ein, um sicherzustellen, dass alle im Rahmen dieses Vertrags verarbeiteten personenbezogenen Daten dem Zweck angemessen und dafür erheblich sind, nicht über das erforderliche Maß hinausgehen, richtig sind und nicht länger als notwendig aufbewahrt werden.

3.3 Der Verantwortliche kann den Auftragsverarbeiter durch dokumentierte Anweisungen bevollmächtigen, personenbezogene Daten mit den folgenden Kategorien von Dritten zu teilen, die jeweils als eigenständige Verantwortliche in Bezug auf die von ihnen empfangenen personenbezogenen Daten handeln:

(a) vom Verantwortlichen beauftragte Unternehmen für professionelle Überwachung und Alarmempfangszentrale (NSL);

(b) vom Verantwortlichen beauftragte Sicherheits- und Wachdienste;

(c) Errichter- und Wartungsingenieure, denen der Verantwortliche Zugriffsrechte für das PRO-Konto gewährt hat.

Der Auftragsverarbeiter übermittelt personenbezogene Daten an solche Dritte nur auf dokumentierte Anweisung des Verantwortlichen und übernimmt keine Verantwortung für deren spätere Verarbeitung.

3.4 Der Auftragsverarbeiter wird hiermit ermächtigt, direkt auf Anfragen von betroffenen Personen bezüglich der Ausübung ihrer Rechte gemäß den geltenden Datenschutzbestimmungen im Zusammenhang mit der Verarbeitung im Rahmen dieses Vertrags zu antworten. Der Auftragsverarbeiter informiert den Verantwortlichen über jede solche Anfrage und die ergriffenen inhaltlichen Maßnahmen spätestens innerhalb von fünf (5) Werktagen nach Bearbeitung der Anfrage. Die Unterstützungspflicht des Auftragsverarbeiters beschränkt sich unter Berücksichtigung der Art der Verarbeitung auf Maßnahmen,

die technisch machbar sind.

3.5 Der Auftragsverarbeiter bietet dem Verantwortlichen ferner kaufmännisch angemessene Unterstützung bei der Gewährleistung der Einhaltung der Verpflichtungen des Verantwortlichen zur Durchführung von Sicherheits- und Datenschutz-Folgenabschätzungen, zur Meldung von Datenschutzverletzungen und zur Durchführung vorheriger Konsultationen mit der zuständigen Aufsichtsbehörde, wie im geltenden Datenschutzrecht vorgesehen, unter Berücksichtigung der Art der Verarbeitung und der dem Auftragsverarbeiter zur Verfügung stehenden Informationen.

3.6 Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der vom Auftragsverarbeiter im Rahmen dieses Vertrags durchgeführten Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen ergreift der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um die personenbezogenen Daten vor unbefugter und unrechtmäßiger Verarbeitung sowie vor versehentlichem Verlust, Veränderung oder Zerstörung zu schützen.

3.7 Diese Maßnahmen umfassen, soweit angemessen und für den jeweiligen Verarbeitungsvorgang relevant:

i. die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

ii. die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

iii. die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

iv. ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

3.8 Darüber hinaus stellt der Auftragsverarbeiter sicher und sorgt dafür, dass sein Personal:

i. dem Verantwortlichen unverzüglich alle Informationen zur Verfügung stellt, die der Verantwortliche benötigt, um seinen Verpflichtungen in Bezug auf die Rechte der betroffenen Personen, einschließlich des Auskunftsrechts, nachzukommen oder um Mitteilungen und Anfragen von Datenschutzbehörden zu beantworten;

ii. sicherstellt, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen; und

iii. den Verantwortlichen unverzüglich über Anfragen von betroffenen Personen, dem Datenschutz-Ombudsmann oder einer sonstigen Strafverfolgungs- oder Aufsichtsbehörde informiert.

4. ÜBERMITTLUNG PERSONENBEZOGENER DATEN AUßERHALB DES EWR

4.1 Personenbezogene Daten dürfen ohne vorherige schriftliche Zustimmung des Verantwortlichen nicht außerhalb des Europäischen Wirtschaftsraums übermittelt werden, es sei denn, der Dritte ist an die Standardvertragsklauseln gebunden oder erklärt sich damit einverstanden, an diese gebunden zu sein, oder die Übermittlung fällt unter die in diesem Vertrag festgelegten Fälle, insbesondere in Klausel 4.2.

4.2 Der Verantwortliche wird ferner darüber informiert und erteilt dem Auftragsverarbeiter die Genehmigung, personenbezogene Daten außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums zu übermitteln, um die Bestimmungen und Verpflichtungen dieses Vertrags zu erfüllen. In solchen Fällen verpflichtet sich der Auftragsverarbeiter hiermit, ein hohes Schutzniveau für Übermittlungen personenbezogener Daten außerhalb der EU/des EWR zu gewährleisten, indem er

gegebenenfalls die im Durchführungsbeschluss (EU) 2021/914 der Kommission festgelegten Standardklauseln für internationale Datenübermittlungen in die relevanten Vereinbarungen aufnimmt oder eine andere geeignete Garantie gemäß den Datenschutzbestimmungen umsetzt.

4.3 Jede Bestimmung dieses Vertrags, die dazu führen würde, dass den in Klausel 4.2 genannten Standardklauseln ihre Wirkung als geeignete Garantien gemäß Artikel 46 der DSGVO entzogen wird, findet insoweit keine Anwendung, als sie diese Wirkung hätte.

5. PRÜFUNGEN

5.1 Gemäß Klausel 8.9 der Standardvertragsklauseln vereinbaren die Parteien die folgenden Modalitäten für die Ausübung von Prüfungsrechten im Rahmen dieses Vertrags:

i. zur Durchführung einer Prüfung im Rahmen dieses Vertrags beauftragen die Parteien ausschließlich unabhängige Prüfer, die eine Vertraulichkeitsvereinbarung mit dem Auftragsverarbeiter unterzeichnen müssen;
ii. die Prüfung umfasst keinen Zugang zu den Räumlichkeiten oder Informationssystemen des Auftragsverarbeiters und wird ausschließlich in dokumentarischer Form durchgeführt;
iii. die Prüfung darf nicht öfter als einmal pro Jahr nach schriftlicher Benachrichtigung des Auftragsverarbeiters mindestens dreißig (30) Kalendertage vor dem geplanten Beginn der Prüfung durchgeführt werden;
iv. alle Kosten einer solchen Prüfung sind vom Verantwortlichen vollständig zu tragen; und
v. eine Prüfung durch den Verantwortlichen schränkt die Pflichten und die Haftung des Auftragsverarbeiters im Rahmen dieses Vertrags in keiner Weise ein.

5.2 Nichts in diesem Abschnitt ist so auszulegen, dass es die Rechte des Verantwortlichen gemäß Klausel 8.9 der Standardvertragsklauseln einschränkt oder begrenzt. Die in diesem Abschnitt festgelegten Verfahren stellen die praktischen Modalitäten dar, über die diese Rechte gewöhnlich ausgeübt werden.

6. VERLETZUNGEN

6.1 Der Auftragsverarbeiter benachrichtigt den Verantwortlichen unverzüglich, spätestens jedoch innerhalb von zweiundsiebzig (72) Stunden, nachdem ihm eine Verletzung der Sicherheit bekannt geworden ist, die zur zufälligen oder unrechtmäßigen Zerstörung, zum Verlust, zur Veränderung, zur unbefugten Offenlegung von oder zum unbefugten Zugriff auf personenbezogene Daten führt, die im Auftrag des Verantwortlichen verarbeitet werden („**Verletzung**“). Hat der Auftragsverarbeiter begründeten Anlass zu der Annahme, dass eine solche Verletzung aufgetreten ist, informiert er den Verantwortlichen entsprechend. Der Auftragsverarbeiter benachrichtigt im Namen des Verantwortlichen weder eine Aufsichtsbehörde noch eine betroffene Person über eine Verletzung, es sei denn, er wird vom Verantwortlichen schriftlich dazu angewiesen oder ist nach geltendem Recht dazu verpflichtet.

6.2 Der Auftragsverarbeiter stellt dem Verantwortlichen alle relevanten Informationen bezüglich der Verletzung zur Verfügung. Die Benachrichtigung des Verantwortlichen über die Verletzung durch den Auftragsverarbeiter umfasst mindestens Folgendes:

i. eine Beschreibung der Art der Verletzung und der davon betroffenen Informationen;

ii. den Namen und die Kontaktdaten der Ansprechstelle des Auftragsverarbeiters, bei der weitere Informationen eingeholt werden können;

iii. eine Beschreibung der vom Auftragsverarbeiter ergriffenen Maßnahmen zur Behebung der Verletzung, einschließlich gegebenenfalls von Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

6.3 Der Auftragsverarbeiter dokumentiert alle Verletzungen, einschließlich der mit jeder Verletzung zusammenhängenden Tatsachen, ihrer Auswirkungen und der ergriffenen Abhilfemaßnahmen.

7. EINBINDUNG DRITTER BEI DER DATENVERARBEITUNG

7.1 **Allgemeine Genehmigung.** Der Verantwortliche erteilt seine allgemeine Genehmigung dazu, dass der Auftragsverarbeiter verbundene Unternehmen des Auftragsverarbeiters und sonstige Subunternehmer als Unterauftragsverarbeiter zur Verarbeitung personenbezogener Daten im Zusammenhang mit den Diensten hinzuzieht („**Unterauftragsverarbeiter**"), vorausgesetzt, dass eine solche Beauftragung nicht zur Nichteinhaltung geltenden Rechts oder der Pflichten des Auftragsverarbeiters aus diesem Vertrag führt. Der Auftragsverarbeiter führt eine Liste der von ihm eingesetzten Unterauftragsverarbeiter im Ajax DSGVO Whitepaper (FAQ) unter https://ajax.systems/gdpr-white-paper/. Der Auftragsverarbeiter stellt sicher, dass die hinzugezogenen Unterauftragsverarbeiter ordnungsgemäß qualifiziert und vertraglich an Datenschutzpflichten gebunden sind, die nicht weniger schützend sind als die in diesem Vertrag festgelegten, sei es durch einen Auftragsverarbeitungsvertrag oder eine sonstige verbindliche Vertragsdokumentation.

7.2 **Wechsel von Unterauftragsverarbeitern.** Gemäß Klausel 9 der in Anlage 1 enthaltenen Standardvertragsklauseln wird die Pflicht des Auftragsverarbeiters, den Verantwortlichen über die Hinzufügung oder den Austausch eines Unterauftragsverarbeiters zu informieren, dadurch erfüllt, dass die im Ajax DSGVO Whitepaper (FAQ) unter https://ajax.systems/gdpr-white-paper/ veröffentlichte Liste der Unterauftragsverarbeiter aktualisiert wird und der Verantwortliche per E-Mail an die im Konto des Verantwortlichen registrierte Adresse und/oder durch eine Benachrichtigung innerhalb der Produkte und Software von Ajax benachrichtigt wird. Eine solche Benachrichtigung erfolgt mindestens fünf (5) Werktage, bevor der neue oder ersetzende Unterauftragsverarbeiter mit der Verarbeitung personenbezogener Daten im Rahmen dieses Vertrags beginnt. Der Verantwortliche kann einer solchen Änderung innerhalb dieser Frist durch schriftliche Mitteilung an den Auftragsverarbeiter widersprechen. Geht bis zum Ablauf dieser Frist kein Widerspruch ein, gilt die Änderung als genehmigt.

8. LÖSCHUNG UND RÜCKGABE PERSONENBEZOGENER DATEN

8.1 Nach Beendigung oder Ablauf der Endanwendervereinbarung, Schließung des Kontos des Verantwortlichen oder auf Aufforderung des Verantwortlichen hat der Auftragsverarbeiter nach Wahl des Verantwortlichen alle im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten zu löschen oder an den Verantwortlichen zurückzugeben und bestehende Kopien zu löschen, es sei denn, nach geltendem Recht ist eine weitere Speicherung erforderlich. Der Verantwortliche kann seine Wahl jederzeit vor dem Ende der Erbringung der Dienstleistungen durch schriftliche Mitteilung an den Auftragsverarbeiter ändern.

8.2 Hat der Verantwortliche seine Wahl gemäß Klausel 8.1 nicht innerhalb von dreißig (30) Kalendertagen nach dem entsprechenden Ereignis mitgeteilt, löscht der Auftragsverarbeiter die personenbezogenen Daten.

8.3 Die Löschung aus den aktiven Produktionssystemen des Auftragsverarbeiters muss innerhalb von dreißig (30) Kalendertagen ab dem Datum der entsprechenden Aufforderung bzw. des in Klausel 8.1 genannten Ereignisses abgeschlossen sein.

8.4 Personenbezogene Daten können nach der Löschung gemäß Klausel 8.3 für die Dauer des Backup-Aufbewahrungszyklus des Auftragsverarbeiters, der zwölf (12) Monate nicht überschreitet, in verschlüsselten Sicherungskopien verbleiben. Während dieses Zeitraums werden diese personenbezogenen Daten für keinen anderen Zweck verarbeitet, der Zugriff darauf wird beschränkt, und sie werden nach Ablauf des jeweiligen Backup-Zyklus dauerhaft gelöscht. Im Falle einer Wiederherstellung aus einem Backup entfernt der Auftragsverarbeiter die personenbezogenen Daten von Verantwortlichen, deren Daten zuvor gelöscht wurden, bevor die wiederhergestellten Daten in der

Produktion verwendet werden.

8.5 Bis zum Abschluss der Löschung oder Rückgabe stellt der Auftragsverarbeiter weiterhin die Einhaltung dieses Vertrags in Bezug auf die betreffenden personenbezogenen Daten sicher.

8.6 Der Auftragsverarbeiter bestätigt dem Verantwortlichen auf dessen Aufforderung schriftlich, dass die Löschung abgeschlossen ist.

8.7 Soweit geltendes Recht vom Auftragsverarbeiter verlangt, personenbezogene Daten über die in diesem Abschnitt festgelegten Fristen hinaus aufzubewahren, informiert der Auftragsverarbeiter den Verantwortlichen über dieses Erfordernis, es sei denn, dies ist ihm gesetzlich verboten, und verarbeitet die aufbewahrten personenbezogenen Daten nur in dem Umfang und so lange wie erforderlich.

9. KÜNDIGUNG UND SONSTIGES

9.1 Dieser Vertrag tritt gleichzeitig mit der Endanwendervereinbarung in Kraft und bildet ab dem Datum, an dem der Verantwortliche die Endanwendervereinbarung unter https://ajax.systems/end-user-agreement/ akzeptiert, einen wesentlichen Bestandteil derselben. Dieser Vertrag bleibt so lange in Kraft, bis der Auftragsverarbeiter die Verarbeitung personenbezogener Daten auf der Grundlage der Dienstleistungen oder einer Vereinbarung zwischen den Parteien eingestellt und die Pflichten im Zusammenhang mit dem Abschluss der Verarbeitung erfüllt hat, sofern zwischen den Parteien nicht schriftlich etwas anderes vereinbart wurde.

9.2 Die Kündigung oder das Erlöschen dieses Vertrags entbindet die Parteien nicht von Vertraulichkeitspflichten oder sonstigen Verantwortlichkeiten im Rahmen dieses Vertrags.

9.3 Ajax kann diesen Vertrag durch Veröffentlichung einer aktualisierten Version auf der Ajax Website, durch E-Mail-Benachrichtigung oder durch eine Benachrichtigung innerhalb der Produkte und/oder mobilen Anwendungen ändern. Die fortgesetzte Nutzung der Produkte oder Software nach einer solchen Benachrichtigung gilt als Zustimmung zum geänderten Vertrag. Dieses Änderungsrecht erstreckt sich nicht auf die Standardvertragsklauseln in Anlage 1, die nur so aktualisiert werden dürfen, wie es im Rahmen dieser Klauseln zulässig ist.

10. ANWENDBARES RECHT UND BEILEGUNG VON STREITIGKEITEN

10.1 Dieser Vertrag einschließlich aller Anlagen, Anhänge und sonstiger wesentlicher Bestandteile unterliegt dem Recht der Republik Polen und ist nach diesem auszulegen.

10.2 Die Parteien vereinbaren ferner, das anwendbare Datenschutzrecht bezüglich der Verarbeitung personenbezogener Daten einzuhalten.

10.3 „Anwendbares Datenschutzrecht“ bezeichnet die jeweils geltenden Rechtsvorschriften zur Verarbeitung personenbezogener Daten, einschließlich der Datenschutz-Grundverordnung (EU) 2016/679, des UK Data Protection Act 2018, der Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG (in der durch die Richtlinie 2009/136/EG aktualisierten Fassung), der Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) in der jeweils gültigen Fassung sowie aller sonstigen EWR-Rechtsvorschriften über personenbezogene Daten und aller sonstigen jeweils geltenden Rechtsvorschriften und behördlichen Anforderungen, die für die Parteien in Bezug auf die Nutzung personenbezogener Daten gelten (einschließlich, aber nicht beschränkt auf den Schutz der Daten in der elektronischen Kommunikation), abhängig von dem Gebiet, in dem die Produkte und die Software bereitgestellt werden.

10.4 Alle Streitigkeiten, Meinungsverschiedenheiten oder Ansprüche, die sich aus oder im

Zusammenhang mit diesem Vertrag ergeben, sowie bezüglich dessen Auslegung, Durchsetzbarkeit, Erfüllung, Verletzung, Beendigung oder Gültigkeit, werden vor den Gerichten Polens (Warschau) beigelegt, sofern das anwendbare Datenschutzrecht nichts anderes vorsieht. Die Verfahrenssprache ist Englisch.

10.5 Die Parteien vereinbaren unwiderruflich, dass die Gerichte der Republik Polen die ausschließliche Zuständigkeit für die Beilegung aller Streitigkeiten haben, die sich aus oder im Zusammenhang mit dem Vertrag ergeben, insbesondere Streitigkeiten bezüglich seiner Erfüllung, seines Bestehens, seiner Gültigkeit, Auslegung, Beendigung oder seiner Folgen. Dementsprechend sind alle Klagen oder Verfahren, die sich aus oder im Zusammenhang mit dem Vertrag ergeben, unabhängig davon, ob sie auf vertraglicher oder außervertraglicher Haftung beruhen, ausschließlich vor den Gerichten der Republik Polen zu erheben. Ist der Verantwortliche eine natürliche Person, die als einzelner Endnutzer handelt (wie in der Endanwendervereinbarung definiert), kann der Verantwortliche Verfahren auch vor den Gerichten seines Landes des gewöhnlichen Aufenthalts anstrengen.

Anlage 1. STANDARDVERTRAGSKLAUSELN

ABSCHNITT I

Klausel 1

Zweck und Anwendungsbereich

(a) Mit diesen Standardvertragsklauseln soll sichergestellt werden, dass die Anforderungen der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) bei der Übermittlung personenbezogener Daten an ein Drittland eingehalten werden.

(b) Die Parteien:

(i) die in Anhang 1 aufgeführte(n) natürliche(n) oder juristische(n) Person(en), Behörde(n), Agentur(en) oder sonstige(n) Stelle(n) (im Folgenden „Einrichtung(en)“), die die personenbezogenen Daten übermittelt/n (im Folgenden jeweils „Datenexporteur“), und

(ii) die in Anhang 1 aufgeführte(n) Einrichtung(en) in einem Drittland, die die personenbezogenen Daten direkt oder indirekt über eine andere Einrichtung, die ebenfalls Partei dieser Klauseln ist, erhält/erhalten (im Folgenden jeweils „Datenimporteur“), haben sich mit diesen Standardvertragsklauseln (im Folgenden „Klauseln“) einverstanden erklärt.

(c) Diese Klauseln gelten für die Übermittlung personenbezogener Daten gemäß Anhang 1.

(d) Die Anlage zu diesen Klauseln mit den darin enthaltenen Anhängen ist Bestandteil dieser Klauseln.

Klausel 2

Wirkung und Unabänderbarkeit der Klauseln

(a) Diese Klauseln enthalten geeignete Garantien, einschließlich durchsetzbarer Rechte betroffener Personen und wirksamer Rechtsbehelfe gemäß Artikel 46 Absatz (1) und Artikel 46 Absatz (2) Buchstabe (c) der Verordnung (EU) 2016/679 sowie — in Bezug auf Datenübermittlungen von Verantwortlichen an Auftragsverarbeiter und/oder von Auftragsverarbeitern an Auftragsverarbeiter — Standardvertragsklauseln gemäß Artikel 28 Absatz (7) der Verordnung (EU) 2016/679, sofern diese nicht geändert werden, mit Ausnahme der Auswahl des entsprechenden Moduls oder der entsprechenden Module oder der Ergänzung oder Aktualisierung von Informationen in der Anlage. Dies hindert die Parteien nicht daran, die in diesen Klauseln festgelegten Standardvertragsklauseln in einen umfangreicheren Vertrag aufzunehmen und/oder weitere Klauseln oder zusätzliche Garantien hinzuzufügen, sofern diese weder unmittelbar noch mittelbar im Widerspruch zu diesen Klauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden.

(b) Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Datenexporteur gemäß der Verordnung (EU) 2016/679 unterliegt.

Klausel 3

Drittbegünstigte

(a) Betroffene Personen können diese Klauseln als Drittbegünstigte gegenüber dem Datenexporteur und/oder dem Datenimporteur geltend machen und durchsetzen, mit folgenden Ausnahmen:

(i) Klausel 1, Klausel 2, Klausel 3, Klausel 6, Klausel 7;

(ii) Klausel 8.1 Buchstabe (b), 8.9 Buchstaben (a), (c), (d) und (e);

(iii) Klausel 9 Buchstaben (a), (c), (d) und (e);

(iv) Klausel 12 Buchstaben (a), (d) und (f);

(v) Klausel 13

(vi) Klausel 15.1 Buchstaben (c), (d) und (e);

(vii) Klausel 16 Buchstabe (e);

(viii) Klausel 18 Buchstaben (a) und (b);

(b) Die Rechte betroffener Personen gemäß der Verordnung (EU) 2016/679 bleiben von Buchstabe (a) unberührt.

Klausel 4

Auslegung

(a) Werden in diesen Klauseln in der Verordnung (EU) 2016/679 definierte Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in dieser Verordnung.

(b) Diese Klauseln sind im Lichte der Bestimmungen der Verordnung (EU) 2016/679 auszulegen.

(c) Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die mit den in der Verordnung (EU) 2016/679 vorgesehenen Rechten und Pflichten im Widerspruch steht.

Klausel 5

Vorrang

Im Falle eines Widerspruchs zwischen diesen Klauseln und den Bestimmungen von damit zusammenhängenden Vereinbarungen zwischen den Parteien, die zu dem Zeitpunkt bestehen, zu dem diese Klauseln vereinbart oder eingegangen werden, haben diese Klauseln Vorrang.

Klausel 6

Beschreibung der Datenübermittlung(en)

Die Einzelheiten der Datenübermittlung(en), insbesondere die Kategorien der übermittelten personenbezogenen Daten und der/die Zweck(e), zu dem/denen sie übermittelt werden, sind in Anhang 1 aufgeführt.

Klausel 7

Kopplungsklausel

Die optionale Kopplungsklausel findet in Klausel 7 keine Anwendung.

ABSCHNITT II — PFLICHTEN DER PARTEIEN

Klausel 8

Datenschutzgarantien

Der Datenexporteur versichert, sich im Rahmen des Zumutbaren davon überzeugt zu haben, dass der Datenimporteur — durch die Umsetzung geeigneter technischer und organisatorischer Maßnahmen — in der Lage ist, seinen Pflichten aus diesen Klauseln nachzukommen.

8.1. Weisungen

(a) Der Datenimporteur verarbeitet die personenbezogenen Daten nur auf dokumentierte Weisung des Datenexporteurs. Der Datenexporteur kann solche Weisungen während der gesamten Vertragslaufzeit erteilen.

(b) Der Datenimporteur unterrichtet den Datenexporteur unverzüglich, wenn er diese Weisungen nicht befolgen kann.

8.2. Zweckbindung

Der Datenimporteur verarbeitet die personenbezogenen Daten nur für den/die in Anhang 1 genannten spezifischen Zweck(e), sofern keine weiteren Weisungen des Datenexporteurs bestehen.

8.3. Transparenz

Auf Anfrage stellt der Datenexporteur der betroffenen Person eine Kopie dieser Klauseln, einschließlich der von den Parteien ausgefüllten Anlage, unentgeltlich zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich der in Anhang 2 beschriebenen Maßnahmen und personenbezogener Daten, notwendig ist, kann der Datenexporteur Teile des Textes der Anlage zu diesen Klauseln vor der Weitergabe einer Kopie unkenntlich machen; er legt jedoch eine aussagekräftige Zusammenfassung vor, wenn die betroffene Person andernfalls den Inhalt der Anlage nicht verstehen würde oder ihre Rechte nicht ausüben könnte. Auf Anfrage teilen die Parteien der betroffenen Person die Gründe für die Schwärzungen so weit wie möglich mit, ohne die geschwärzten Informationen offenzulegen. Diese Klausel gilt unbeschadet der Pflichten des Datenexporteurs gemäß den Artikeln 13 und 14 der Verordnung (EU) 2016/679.

8.4. Richtigkeit

Stellt der Datenimporteur fest, dass die erhaltenen personenbezogenen Daten unrichtig oder veraltet sind, unterrichtet er unverzüglich den Datenexporteur. In diesem Fall arbeitet der Datenimporteur mit dem Datenexporteur zusammen, um die Daten zu löschen oder zu berichtigen.

8.5. Dauer der Verarbeitung und Löschung oder Rückgabe der Daten

Die Daten werden vom Datenimporteur nur für die in Anhang 1 angegebene Dauer verarbeitet. Nach Wahl des Datenexporteurs löscht der Datenimporteur nach Beendigung der Erbringung der Datenverarbeitungsdienste alle im Auftrag des Datenexporteurs verarbeiteten personenbezogenen Daten und bescheinigt dem Datenexporteur, dass dies erfolgt ist, oder gibt dem Datenexporteur alle in seinem Auftrag verarbeiteten personenbezogenen Daten zurück und löscht bestehende Kopien. Bis zur Löschung oder Rückgabe der Daten stellt der Datenimporteur weiterhin die Einhaltung dieser Klauseln sicher. Falls für den Datenimporteur lokale Rechtsvorschriften gelten, die ihm die Rückgabe oder Löschung der personenbezogenen Daten untersagen, sichert der Datenimporteur zu, dass er die Einhaltung dieser Klauseln auch weiterhin gewährleistet und diese Daten nur in dem Umfang und so lange verarbeitet, wie dies gemäß den betreffenden lokalen Rechtsvorschriften erforderlich ist. Dies gilt unbeschadet von Klausel 14, insbesondere der Pflicht des Datenimporteurs gemäß Klausel 14 Buchstabe (e), den Datenexporteur während der Vertragslaufzeit zu benachrichtigen, wenn er Grund zu

der Annahme hat, dass für ihn Rechtsvorschriften oder Gepflogenheiten gelten oder gelten werden, die nicht mit den Anforderungen in Klausel 14 Buchstabe (a) im Einklang stehen.

8.6. Sicherheit der Verarbeitung

(a) Der Datenimporteur und, während der Datenübermittlung, auch der Datenexporteur treffen geeignete technische und organisatorische Maßnahmen, um die Sicherheit der Daten zu gewährleisten, einschließlich des Schutzes vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu diesen Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten"). Bei der Beurteilung des angemessenen Schutzniveaus tragen die Parteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und dem/den Zweck(en) der Verarbeitung sowie den mit der Verarbeitung verbundenen Risiken für die betroffenen Personen gebührend Rechnung. Die Parteien ziehen insbesondere eine Verschlüsselung oder Pseudonymisierung, auch während der Datenübermittlung, in Betracht, wenn dadurch der Verarbeitungszweck erfüllt werden kann. Im Falle einer Pseudonymisierung verbleiben die zusätzlichen Informationen, mit denen die personenbezogenen Daten einer speziellen betroffenen Person zugeordnet werden können, soweit möglich, unter der ausschließlichen Kontrolle des Datenexporteurs. Zur Erfüllung seinen Pflichten gemäß diesem Absatz setzt der Datenimporteur mindestens die in Anhang 2 aufgeführten technischen und organisatorischen Maßnahmen um. Der Datenimporteur führt regelmäßige Kontrollen durch, um sicherzustellen, dass diese Maßnahmen weiterhin ein angemessenes Schutzniveau bieten.

(b) Der Datenimporteur gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Er gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

(c) Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Datenimporteur gemäß diesen Klauseln ergreift der Datenimporteur geeignete Maßnahmen zur Behebung der Verletzung, darunter auch Maßnahmen zur Abmilderung ihrer nachteiligen Auswirkungen. Zudem meldet der Datenimporteur dem Datenexporteur die Verletzung unverzüglich, nachdem sie ihm bekannt wurde. Diese Meldung enthält die Kontaktdaten einer Anlaufstelle für weitere Informationen, eine Beschreibung der Art der Verletzung (soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen personenbezogenen Datensätze), die wahrscheinlichen Folgen der Verletzung und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung etwaiger nachteiliger Auswirkungen. Wenn und soweit nicht alle Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt.

(d) Unter Berücksichtigung der Art der Verarbeitung und der dem Datenimporteur zur Verfügung stehenden Informationen arbeitet der Datenimporteur mit dem Datenexporteur zusammen und unterstützt ihn dabei, seinen Pflichten gemäß der Verordnung (EU) 2016/679 nachzukommen, insbesondere die zuständige Aufsichtsbehörde und die betroffenen Personen zu benachrichtigen.

8.7. Sensible Daten

Soweit die Übermittlung personenbezogene Daten umfasst, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder die genetische Daten oder biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche Verurteilungen und Straftaten enthalten (im Folgenden „sensible Daten“), wendet der Datenimporteur die in Anhang 1 beschriebenen speziellen Beschränkungen und/oder zusätzlichen Garantien an.

8.8. Weiterübermittlungen

Der Datenimporteur gibt die personenbezogenen Daten nur auf dokumentierte Weisung des Datenexporteurs an Dritte weiter. Die Daten dürfen zudem nur an Dritte weitergegeben werden, die (in demselben Land wie der Datenimporteur oder in einem anderen Drittland) außerhalb der Europäischen Union ansässig sind (im Folgenden „Weiterübermittlung“), sofern der Dritte im Rahmen des betreffenden Moduls an diese Klauseln gebunden ist oder sich mit der Bindung daran einverstanden erklärt oder falls

(i) die Weiterübermittlung an ein Land erfolgt, für das ein Angemessenheitsbeschluss nach Artikel 45 der Verordnung (EU) 2016/679 gilt, der die Weiterübermittlung abdeckt,

(ii) der Dritte auf andere Weise geeignete Garantien gemäß Artikel 46 oder Artikel 47 der Verordnung

(EU) 2016/679 im Hinblick auf die betreffende Verarbeitung gewährleistet,

(iii) die Weiterübermittlung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen im Zusammenhang mit bestimmten Verwaltungs-, Gerichts- oder regulatorischen Verfahren erforderlich ist oder

(iv) die Weiterübermittlung erforderlich ist, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen.

Jede Weiterübermittlung erfolgt unter der Bedingung, dass der Datenimporteur alle anderen Garantien gemäß diesen Klauseln, insbesondere die Zweckbindung, einhält.

8.9. Dokumentation und Einhaltung der Klauseln

(a) Der Datenimporteur bearbeitet Anfragen des Datenexporteurs, die sich auf die Verarbeitung gemäß diesen Klauseln beziehen, umgehend und in angemessener Weise.

(b) Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können. Insbesondere führt der Datenimporteur geeignete Aufzeichnungen über die im Auftrag des Datenexporteurs durchgeführten Verarbeitungstätigkeiten.

(c) Der Datenimporteur stellt dem Datenexporteur alle Informationen zur Verfügung, die erforderlich sind, um die Einhaltung der in diesen Klauseln festgelegten Pflichten nachzuweisen; auf Verlangen des Datenexporteurs ermöglicht er diesem, die unter diese Klauseln fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung zu prüfen, und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Datenexporteur einschlägige Zertifizierungen des Datenimporteurs berücksichtigen.

(d) Der Datenexporteur kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Datenimporteurs umfassen und werden gegebenenfalls mit angemessener Vorankündigung durchgeführt.

(e) Die Parteien stellen der zuständigen Aufsichtsbehörde die unter den Buchstaben (b) und (c) genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

Klausel 9

Einsatz von Unterauftragsverarbeitern

(a) Der Datenimporteur besitzt die allgemeine Genehmigung des Datenexporteurs für die Beauftragung von Unterauftragsverarbeitern, die in einer vereinbarten Liste aufgeführt sind. Der Datenimporteur unterrichtet den Datenexporteur mindestens fünf (5) Werktage im Voraus ausdrücklich in schriftlicher Form über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Datenexporteur damit ausreichend Zeit ein, um vor der Beauftragung des/der Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Der Datenimporteur stellt dem Datenexporteur die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann.

(b) Beauftragt der Datenimporteur einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Datenexporteurs), so muss diese Beauftragung im Wege eines schriftlichen Vertrags erfolgen, der im Wesentlichen dieselben Datenschutzpflichten vorsieht wie diejenigen, die den Datenimporteur gemäß diesen Klauseln binden, einschließlich im Hinblick auf Rechte als Drittbegünstigte für betroffene Personen. Die Parteien erklären sich damit einverstanden, dass der Datenimporteur durch Einhaltung der vorliegenden Klausel seinen Pflichten gemäß Klausel 8.8 nachkommt. Der Datenimporteur stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Datenimporteur gemäß diesen Klauseln unterliegt.

(c) Der Datenimporteur stellt dem Datenexporteur auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten, notwendig ist, kann der Datenimporteur den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.

(d) Der Datenimporteur haftet gegenüber dem Datenexporteur in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Datenimporteur geschlossenen Vertrag nachkommt. Der Datenimporteur benachrichtigt den Datenexporteur, wenn der Unterauftragsverarbeiter seinen Pflichten gemäß diesem Vertrag nicht nachkommt.

(e) Der Datenimporteur vereinbart mit dem Unterauftragsverarbeiter eine Drittbegünstigtenklausel, wonach der Datenexporteur — sollte der Datenimporteur faktisch oder rechtlich nicht mehr bestehen oder zahlungsunfähig sein — das Recht hat, den Untervergabevertrag zu kündigen und den Unterauftragsverarbeiter anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben.

Klausel 10

Rechte betroffener Personen

(a) Der Datenimporteur unterrichtet den Datenexporteur unverzüglich über jeden Antrag, den er von einer betroffenen Person erhalten hat. Er beantwortet diesen Antrag nicht selbst, es sei denn, er wurde vom Datenexporteur dazu ermächtigt.

(b) Der Datenimporteur unterstützt den Datenexporteur bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte gemäß der Verordnung (EU) 2016/679 zu beantworten. Zu diesem Zweck legen die Parteien in Anhang 2 unter Berücksichtigung der Art der Verarbeitung die geeigneten technischen und organisatorischen Maßnahmen, durch die Unterstützung geleistet wird, sowie den Anwendungsbereich und den Umfang der erforderlichen Unterstützung fest.

(c) Bei der Erfüllung seiner Pflichten gemäß den Buchstaben (a) und (b) befolgt der Datenimporteur die Weisungen des Datenexporteurs.

Klausel 11

Rechtsbehelf

(a) Der Datenimporteur informiert die betroffenen Personen in transparenter und leicht zugänglicher Form mittels individueller Benachrichtigung oder auf seiner Website über eine Anlaufstelle, die befugt ist, Beschwerden zu bearbeiten. Er bearbeitet umgehend alle Beschwerden, die er von einer betroffenen Person erhält.

(b) Im Falle einer Streitigkeit zwischen einer betroffenen Person und einer der Parteien bezüglich der Einhaltung dieser Klauseln bemüht sich die betreffende Partei nach besten Kräften um eine zügige gütliche Beilegung. Die Parteien halten einander über derartige Streitigkeiten auf dem Laufenden und bemühen sich gegebenenfalls gemeinsam um deren Beilegung.

(c) Macht die betroffene Person ein Recht als Drittbegünstigte gemäß Klausel 3 geltend, erkennt der Datenimporteur die Entscheidung der betroffenen Person an,

(i) eine Beschwerde bei der Aufsichtsbehörde des Mitgliedstaats ihres gewöhnlichen Aufenthaltsorts oder ihres Arbeitsorts oder bei der zuständigen Aufsichtsbehörde gemäß Klausel 13 einzureichen,

(ii) den Streitfall an die zuständigen Gerichte im Sinne der Klausel 18 zu verweisen.

(d) Die Parteien erkennen an, dass die betroffene Person von einer Einrichtung, Organisation oder Vereinigung ohne Gewinnerzielungsabsicht gemäß Artikel 80 Absatz (1) der Verordnung (EU) 2016/679 vertreten werden kann.

(e) Der Datenimporteur unterwirft sich einem nach geltendem Unionsrecht oder dem geltenden Recht eines Mitgliedstaats verbindlichen Beschluss.

(f) Der Datenimporteur erklärt sich damit einverstanden, dass die Entscheidung der betroffenen Person nicht ihre materiellen Rechte oder Verfahrensrechte berührt, Rechtsbehelfe im Einklang mit geltenden Rechtsvorschriften einzulegen.

Klausel 12

Haftung

(a) Jede Partei haftet gegenüber der/den anderen Partei(en) für Schäden, die sie der/den anderen Partei(en) durch einen Verstoß gegen diese Klauseln verursacht.

(b) Der Datenimporteur haftet gegenüber der betroffenen Person, und die betroffene Person hat Anspruch auf Schadenersatz für jeden materiellen oder immateriellen Schaden, den der Datenimporteur oder sein Unterauftragsverarbeiter der betroffenen Person verursacht, indem er deren Rechte als Drittbegünstigte gemäß diesen Klauseln verletzt.

(c) Ungeachtet von Buchstabe (b) haftet der Datenimporteur gegenüber der betroffenen Person, und die betroffene Person hat Anspruch auf Schadenersatz für jeden materiellen oder immateriellen Schaden, den der Datenexporteur oder der Datenimporteur (oder dessen Unterauftragsverarbeiter) der betroffenen Person verursacht, indem er deren Rechte als Drittbegünstigte gemäß diesen Klauseln verletzt. Dies gilt unbeschadet der Haftung des Datenexporteurs und, sofern der Datenexporteur ein im Auftrag eines Verantwortlichen handelnder Auftragsverarbeiter ist, unbeschadet der Haftung des Verantwortlichen gemäß der Verordnung (EU) 2016/679 oder gegebenenfalls der Verordnung (EU) 2018/1725.

(d) Die Parteien erklären sich damit einverstanden, dass der Datenexporteur, der nach Buchstabe (c) für durch den Datenimporteur (oder dessen Unterauftragsverarbeiter) verursachte Schäden haftet, berechtigt ist, vom Datenimporteur den Teil des Schadenersatzes zurückzufordern, der der Verantwortung des Datenimporteurs für den Schaden entspricht.

(e) Ist mehr als eine Partei für Schäden verantwortlich, die der betroffenen Person infolge eines Verstoßes gegen diese Klauseln entstanden sind, so haften alle verantwortlichen Parteien gesamtschuldnerisch, und die betroffene Person ist berechtigt, gegen jede der Parteien gerichtlich vorzugehen.

(f) Die Parteien erklären sich damit einverstanden, dass eine Partei, die nach Buchstabe (e) haftbar gemacht wird, berechtigt ist, von der/den anderen Partei(en) den Teil des Schadenersatzes zurückzufordern, der deren Verantwortung für den Schaden entspricht.

(g) Der Datenimporteur kann sich nicht auf das Verhalten eines Unterauftragsverarbeiters berufen, um sich seiner eigenen Haftung entziehen.

Klausel 13

Aufsicht

(a) Die Aufsichtsbehörde, die dafür verantwortlich ist, sicherzustellen, dass der Datenexporteur bei Datenübermittlungen die Verordnung (EU) 2016/679 einhält, fungiert als zuständige Aufsichtsbehörde (entsprechend der Angabe in Anhang 1).

(b) Der Datenimporteur erklärt sich damit einverstanden, sich der Zuständigkeit der zuständigen Aufsichtsbehörde zu unterwerfen und bei allen Verfahren, mit denen die Einhaltung dieser Klauseln sichergestellt werden soll, mit ihr zusammenzuarbeiten. Insbesondere erklärt sich der Datenimporteur damit einverstanden, Anfragen zu beantworten, sich Prüfungen zu unterziehen und den von der Aufsichtsbehörde getroffenen Maßnahmen, darunter auch Abhilfemaßnahmen und Ausgleichsmaßnahmen, nachzukommen. Er bestätigt der Aufsichtsbehörde in schriftlicher Form, dass die erforderlichen Maßnahmen ergriffen wurden.

ABSCHNITT III — LOKALE RECHTSVORSCHRIFTEN UND PFLICHTEN IM FALLE DES ZUGANGS VON BEHÖRDEN ZU DEN DATEN

Klausel 14

Lokale Rechtsvorschriften und Gepflogenheiten, die sich auf die Einhaltung der Klauseln auswirken

(a) Die Parteien sichern zu, keinen Grund zu der Annahme zu haben, dass die für die Verarbeitung personenbezogener Daten durch den Datenimporteur geltenden Rechtsvorschriften und Gepflogenheiten im Bestimmungsdrittland, einschließlich Anforderungen zur Offenlegung personenbezogener Daten oder Maßnahmen, die öffentlichen Behörden den Zugang zu diesen Daten gestatten, den Datenimporteur an der Erfüllung seiner Pflichten gemäß diesen Klauseln hindern. Dies basiert auf dem Verständnis, dass Rechtsvorschriften und Gepflogenheiten, die den Wesensgehalt der Grundrechte und Grundfreiheiten achten und nicht über Maßnahmen hinausgehen, die in einer demokratischen Gesellschaft notwendig und verhältnismäßig sind, um eines der in Artikel 23 Absatz (1) der Verordnung (EU) 2016/679 aufgeführten Ziele sicherzustellen, nicht im Widerspruch zu diesen Klauseln stehen.

(b) Die Parteien erklären, dass sie hinsichtlich der Zusicherung in Buchstabe (a) insbesondere die folgenden Aspekte gebührend berücksichtigt haben:

(i) die besonderen Umstände der Übermittlung, einschließlich der Länge der Verarbeitungskette, der Anzahl der beteiligten Akteure und der verwendeten Übertragungskanäle, beabsichtigte Datenweiterleitungen, die Art des Empfängers, den Zweck der Verarbeitung, die Kategorien und das Format der übermittelten personenbezogenen Daten, den Wirtschaftszweig, in dem die Übertragung erfolgt, den Speicherort der übermittelten Daten,

(ii) die angesichts der besonderen Umstände der Übermittlung relevanten Rechtsvorschriften und Gepflogenheiten des Bestimmungsdrittlandes (einschließlich solcher, die die Offenlegung von Daten gegenüber Behörden vorschreiben oder den Zugang von Behörden zu diesen Daten

gestatten) sowie die geltenden Beschränkungen und Garantien [1],

(iii) alle relevanten vertraglichen, technischen oder organisatorischen Garantien, die zur Ergänzung der Garantien gemäß diesen Klauseln eingerichtet wurden, einschließlich Maßnahmen, die während der Übermittlung und bei der Verarbeitung personenbezogener Daten im Bestimmungsland angewandt werden.

(c) Der Datenimporteur versichert, dass er sich im Rahmen der Beurteilung nach Buchstabe (b) nach besten Kräften bemüht hat, dem Datenexporteur sachdienliche Informationen zur Verfügung zu stellen, und erklärt sich damit einverstanden, dass er mit dem Datenexporteur weiterhin zusammenarbeiten wird, um die Einhaltung dieser Klauseln zu gewährleisten.

(d) Die Parteien erklären sich damit einverstanden, die Beurteilung nach Buchstabe (b) zu dokumentieren und sie der zuständigen Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen.

(e) Der Datenimporteur erklärt sich damit einverstanden, während der Laufzeit des Vertrags den Datenexporteur unverzüglich zu benachrichtigen, wenn er nach Zustimmung zu diesen Klauseln Grund zu der Annahme hat, dass für ihn Rechtsvorschriften oder Gepflogenheiten gelten, die nicht mit den Anforderungen in Buchstabe (a) im Einklang stehen; hierunter fällt auch eine Änderung der Rechtsvorschriften des Drittlandes oder eine Maßnahme (z. B. ein Offenlegungsersuchen), die sich auf eine nicht mit den Anforderungen in Buchstabe (a) im Einklang stehende Anwendung dieser Rechtsvorschriften in der Praxis bezieht.

[1] Zur Ermittlung der Auswirkungen derartiger Rechtsvorschriften und Gepflogenheiten auf die Einhaltung dieser Klauseln können in die Gesamtbeurteilung verschiedene Elemente einfließen. Diese Elemente können einschlägige und dokumentierte praktische Erfahrungen im Hinblick darauf umfassen, ob es bereits früher Ersuchen um Offenlegung seitens Behörden gab, die einen hinreichend repräsentativen Zeitrahmen abdecken, oder ob es solche Ersuchen nicht gab. Dies betrifft insbesondere interne Aufzeichnungen oder sonstige Belege, die fortlaufend mit gebührender Sorgfalt erstellt und von leitender Ebene bestätigt wurden, sofern diese Informationen rechtmäßig an Dritte weitergegeben werden können. Sofern anhand dieser praktischen Erfahrungen der Schluss gezogen wird, dass dem Datenimporteur die Einhaltung dieser Klauseln nicht unmöglich ist, muss dies durch weitere relevante objektive Elemente untermauert werden; den Parteien obliegt die sorgfältige Prüfung, ob alle diese Elemente ausreichend zuverlässig und repräsentativ sind, um die getroffene Schlussfolgerung zu bekräftigen. Insbesondere müssen die Parteien berücksichtigen, ob ihre praktische Erfahrung durch öffentlich verfügbare oder anderweitig zugängliche zuverlässige Informationen über das Vorhandensein oder Nicht-Vorhandensein von Ersuchen innerhalb desselben Wirtschaftszweigs und/oder über die Anwendung der Rechtsvorschriften in der Praxis, wie Rechtsprechung und Berichte unabhängiger Aufsichtsgremien, erhärtet und nicht widerlegt wird.

(f) Nach einer Benachrichtigung gemäß Buchstabe (e) oder wenn der Datenexporteur anderweitig Grund zu der Annahme hat, dass der Datenimporteur seinen Pflichten gemäß diesen Klauseln nicht mehr nachkommen kann, ermittelt der Datenexporteur unverzüglich geeignete Maßnahmen (z. B. technische oder organisatorische Maßnahmen zur Gewährleistung der Sicherheit und Vertraulichkeit), die der Datenexporteur und/oder der Datenimporteur ergreifen müssen, um Abhilfe zu schaffen. Der Datenexporteur setzt die Datenübermittlung aus, wenn er der Auffassung ist, dass keine geeigneten Garantien für eine derartige Übermittlung gewährleistet werden können, oder wenn er von der dafür zuständigen Aufsichtsbehörde dazu angewiesen wird. In diesem Fall ist der Datenexporteur berechtigt, den Vertrag zu kündigen, soweit es um die Verarbeitung personenbezogener Daten gemäß diesen Klauseln geht. Sind mehr als zwei Parteien an dem Vertrag beteiligt, so kann der Datenexporteur von diesem Kündigungsrecht nur gegenüber der verantwortlichen Partei Gebrauch machen, sofern die Parteien nichts anderes vereinbart haben. Wird der Vertrag gemäß dieser Klausel gekündigt, finden Klausel 16 Buchstaben (d) und (e) Anwendung.

Klausel 15

Pflichten des Datenimporteurs im Falle des Zugangs von Behörden zu den Daten

15.1. Benachrichtigung

(a) Der Datenimporteur erklärt sich damit einverstanden, den Datenexporteur und, soweit möglich, die betroffene Person (gegebenenfalls mit Unterstützung des Datenexporteurs) unverzüglich zu benachrichtigen,

(i) wenn er von einer Behörde, einschließlich Justizbehörden, ein nach den Rechtsvorschriften des Bestimmungslandes rechtlich bindendes Ersuchen um Offenlegung personenbezogener Daten erhält, die gemäß diesen Klauseln übermittelt werden (diese Benachrichtigung muss Informationen über die angeforderten personenbezogenen Daten, die ersuchende Behörde, die Rechtsgrundlage des Ersuchens und die mitgeteilte Antwort enthalten), oder

(ii) wenn er Kenntnis davon erlangt, dass eine Behörde nach den Rechtsvorschriften des Bestimmungslandes direkten Zugang zu personenbezogenen Daten hat, die gemäß diesen Klauseln übermittelt wurden; diese Benachrichtigung muss alle dem Datenimporteur verfügbaren Informationen enthalten.

(b) Ist es dem Datenimporteur gemäß den Rechtsvorschriften des Bestimmungslandes untersagt, den Datenexporteur und/oder die betroffene Person zu benachrichtigen, so erklärt sich der Datenimporteur einverstanden, sich nach besten Kräften um eine Aufhebung des Verbots zu bemühen, damit möglichst viele Informationen so schnell wie möglich mitgeteilt werden können. Der Datenimporteur verpflichtet sich, seine Anstrengungen zu dokumentieren, um diese auf Verlangen des Datenexporteurs nachweisen zu können.

(c) Soweit dies nach den Rechtsvorschriften des Bestimmungslandes zulässig ist, erklärt sich der Datenimporteur bereit, dem Datenexporteur während der Vertragslaufzeit in regelmäßigen Abständen möglichst viele sachdienliche Informationen über die eingegangenen Ersuchen zur Verfügung zu stellen (insbesondere Anzahl der Ersuchen, Art der angeforderten Daten, ersuchende Behörde(n), ob Ersuchen angefochten wurden und das Ergebnis solcher Anfechtungen usw.).

(d) Der Datenimporteur erklärt sich damit einverstanden, die Informationen gemäß den Buchstaben (a) bis (c) während der Vertragslaufzeit aufzubewahren und der zuständigen Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen.

(e) Die Buchstaben (a) bis (c) gelten unbeschadet der Pflicht des Datenimporteurs gemäß Klausel 14 Buchstabe (e) und Klausel 16, den Datenexporteur unverzüglich zu informieren, wenn er diese Klauseln nicht einhalten kann.

15.2. Überprüfung der Rechtmäßigkeit und Datenminimierung

(a) Der Datenimporteur erklärt sich damit einverstanden, die Rechtmäßigkeit des Offenlegungsersuchens zu überprüfen, insbesondere ob das Ersuchen im Rahmen der Befugnisse liegt, die der ersuchenden Behörde übertragen wurden, und das Ersuchen anzufechten, wenn er nach sorgfältiger Beurteilung zu dem Schluss kommt, dass hinreichende Gründe zu der Annahme bestehen, dass das Ersuchen nach den Rechtsvorschriften des Bestimmungslandes, gemäß geltenden völkerrechtlichen Verpflichtungen und nach den Grundsätzen der Völkercourtoisie rechtswidrig ist. Unter den genannten Bedingungen sind vom Datenimporteur mögliche Rechtsmittel einzulegen. Bei der Anfechtung eines Ersuchens erwirkt der Datenimporteur einstweilige Maßnahmen, um die Wirkung des Ersuchens auszusetzen, bis die zuständige Justizbehörde über dessen Begründetheit entschieden hat. Er legt die angeforderten personenbezogenen Daten erst offen, wenn dies nach den geltenden Verfahrensregeln erforderlich ist. Diese Anforderungen gelten unbeschadet der Pflichten des Datenimporteurs gemäß Klausel 14 Buchstabe (e).

(b) Der Datenimporteur erklärt sich damit einverstanden, seine rechtliche Beurteilung und eine etwaige Anfechtung des Offenlegungsersuchens zu dokumentieren und diese Unterlagen dem Datenexporteur zur Verfügung zu stellen, soweit dies nach den Rechtsvorschriften des Bestimmungslandes zulässig ist. Auf Anfrage stellt er diese Unterlagen auch der zuständigen Aufsichtsbehörde zur Verfügung.

(c) Der Datenimporteur erklärt sich damit einverstanden, bei der Beantwortung eines Offenlegungsersuchens auf der Grundlage einer vernünftigen Auslegung des Ersuchens die zulässige Mindestmenge an Informationen bereitzustellen.

ABSCHNITT IV — SCHLUSSBESTIMMUNGEN

Klausel 16

Verstöße gegen die Klauseln und Beendigung des Vertrags

(a) Der Datenimporteur unterrichtet den Datenexporteur unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diese Klauseln einzuhalten.

(b) Verstößt der Datenimporteur gegen diese Klauseln oder kann er diese Klauseln nicht einhalten, setzt der Datenexporteur die Übermittlung personenbezogener Daten an den Datenimporteur aus, bis der Verstoß beseitigt oder der Vertrag beendet ist. Dies gilt unbeschadet von Klausel 14 Buchstabe (f).

(c) Der Datenexporteur ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn

(i) der Datenexporteur die Übermittlung personenbezogener Daten an den Datenimporteur gemäß Buchstabe (b) ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb einer einmonatigen Aussetzung, wiederhergestellt wurde,

(ii) der Datenimporteur in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder

(iii) der Datenimporteur einer verbindlichen Entscheidung eines zuständigen Gerichts oder einer zuständigen Aufsichtsbehörde, die seine Pflichten gemäß diesen Klauseln zum Gegenstand hat, nicht nachkommt.

In diesen Fällen unterrichtet der Datenexporteur die zuständige Aufsichtsbehörde über derartige Verstöße. Sind mehr als zwei Parteien an dem Vertrag beteiligt, so kann der Datenexporteur von diesem Kündigungsrecht nur gegenüber der verantwortlichen Partei Gebrauch machen, sofern die Parteien nichts anderes vereinbart haben.

(d) Personenbezogene Daten, die vor Beendigung des Vertrags gemäß Buchstabe (c) übermittelt wurden, müssen nach Wahl des Datenexporteurs unverzüglich an diesen zurückgegeben oder vollständig gelöscht werden. Dies gilt gleichermaßen für alle Kopien der Daten. Der Datenimporteur bescheinigt dem Datenexporteur die Löschung. Bis zur Löschung oder Rückgabe der Daten stellt der Datenimporteur weiterhin die Einhaltung dieser Klauseln sicher. Falls für den Datenimporteur lokale Rechtsvorschriften gelten, die ihm die Rückgabe oder Löschung der übermittelten personenbezogenen Daten untersagen, sichert der Datenimporteur zu, dass er die Einhaltung dieser Klauseln auch weiterhin gewährleistet und diese Daten nur in dem Umfang und so lange verarbeitet, wie dies gemäß den betreffenden lokalen Rechtsvorschriften erforderlich ist.

(e) Jede Partei kann ihre Zustimmung widerrufen, durch diese Klauseln gebunden zu sein, wenn (i) die Europäische Kommission einen Beschluss nach Artikel 45 Absatz (3) der Verordnung (EU) 2016/679 erlässt, der sich auf die Übermittlung personenbezogener Daten bezieht, für die diese Klauseln gelten, oder (ii) die Verordnung (EU) 2016/679 Teil des Rechtsrahmens des Landes wird, an das die personenbezogenen Daten übermittelt werden. Dies gilt unbeschadet anderer Verpflichtungen, die für die betreffende Verarbeitung gemäß der Verordnung (EU) 2016/679 gelten.

Klausel 17

Anwendbares Recht

Diese Klauseln unterliegen dem Recht eines der EU-Mitgliedstaaten, sofern dieses Recht Rechte als Drittbegünstigte zulässt. Die Parteien vereinbaren, dass dies das Recht von Polen ist.

Klausel 18

Gerichtsstand und Zuständigkeit

(a) Streitigkeiten, die sich aus diesen Klauseln ergeben, werden von den Gerichten eines EU-Mitgliedstaats beigelegt.

(b) Die Parteien vereinbaren, dass dies die Gerichte von Polen sind.

(c) Eine betroffene Person kann Klage gegen den Datenexporteur und/oder den Datenimporteur auch vor den Gerichten des Mitgliedstaats erheben, in dem sie ihren gewöhnlichen Aufenthaltsort hat.

(d) Die Parteien erklären sich damit einverstanden, sich der Zuständigkeit dieser Gerichte zu unterwerfen.

ANHANG 1. BESCHREIBUNG DER DATENVERARBEITUNG

A. LISTE DER PARTEIEN

Datenexporteur

Rolle: Verantwortlicher
Identität und Kontaktdaten: Der Verantwortliche, wie durch die Kontoinformationen (Name oder Firmenname, Adresse und Kontakt-E-Mail) identifiziert, die vom Verantwortlichen in den Produkten und Software von Ajax zum Zeitpunkt der Kontoerstellung registriert wurden.
Für die übermittelten Daten relevante Aktivitäten: Nutzung der Produkte und Software von Ajax zur Sicherung von Räumlichkeiten oder Eigentum unter der Kontrolle des Verantwortlichen.

Datenimporteur

Rolle: Auftragsverarbeiter
Name: AJAX SYSTEMS TRADING FZE
Adresse: S3B2SR06, Jebel Ali Freezone, Dubai, Vereinigte Arabische Emirate
Kontaktdaten: privacy@ajax.systems
Für die übermittelten Daten relevante Aktivitäten: Erbringung von Dienstleistungen, die dem

Verantwortlichen die Nutzung der Produkte und Software von Ajax gemäß der Endanwendervereinbarung ermöglichen.

B. KATEGORIEN BETROFFENER PERSONEN

Die im Rahmen dieser Standardvertragsklauseln übermittelten personenbezogenen Daten betreffen die folgenden Kategorien betroffener Personen:

- der Verantwortliche (Kontoinhaber) und alle Personen, denen der Verantwortliche Kontozugriff gewährt;
- Haushaltsmitglieder, Mitarbeiter, Besucher oder sonstige natürliche Personen, die sich in den Räumlichkeiten oder auf dem Grundstück befinden, die durch die Produkte und Software von Ajax des Verantwortlichen gesichert werden, und deren personenbezogene Daten (einschließlich Bilder und Videoaufnahmen) je nach der vom Verantwortlichen festgelegten Konfiguration erfasst werden können.

C. HÄUFIGKEIT DER ÜBERMITTLUNG

Fortlaufend für die Dauer der Nutzung der Produkte und Software von Ajax durch den Verantwortlichen.

D. GEGENSTAND, ART UND ZWECK DER VERARBEITUNG

Gegenstand, Art und Zwecke der Verarbeitung sind in Abschnitt 2 des Vertrags festgelegt.

E. KATEGORIEN PERSONENBEZOGENER DATEN

Zur Erbringung der in diesem Vertrag festgelegten Dienstleistungen darf der Auftragsverarbeiter folgende Daten verarbeiten:

- Eindeutige Kennungen (Benutzername);
- Informationen über die Nutzung der Produkte und Software von Ajax (wie z. B. Anfragen aus der App);
- IP-Adresse;
- Name, Nachname und Kontaktdaten wie bei der Erstregistrierung angegeben;
- Den Inhalt von SMS-Nachrichten mit Zugangscodes, die während der Registrierung oder bei Kontoänderungen an Endnutzer gesendet werden;
- Informationen über die Mobilgeräte der Endnutzer, einschließlich deren Typ, Betriebssystem und Sprache der Benutzeroberfläche;
- Bild-, Audio- und Videoaufnahmen, die von Produkten und Software von Ajax erfasst wurden;
- Sonstige Daten und Informationen, die bei Bedarf verarbeitet werden.

Besondere Kategorien personenbezogener Daten

Sie werden nicht absichtlich gesammelt. Von den Geräten des Verantwortlichen erfasste Bilder und Videoaufnahmen können beiläufig biometrische Daten (z. B. Gesichtsabbilder) enthalten. Der Auftragsverarbeiter wendet auf all solche Daten die in Anhang 2 beschriebenen zusätzlichen Schutzmaßnahmen an. Daten besonderer Kategorien dürfen nur verarbeitet werden, wenn eine solche Verarbeitung mit den geltenden Datenschutzbestimmungen vereinbar ist und von der betroffenen Person oder dem Verantwortlichen veranlasst wird.

F. DAUER DER VERARBEITUNG / AUFBEWAHRUNG

Für die Dauer der Nutzung der Produkte und Software von Ajax durch den Verantwortlichen. Nach der Beendigung wird die Löschung innerhalb der in Abschnitt 8 des Vertrags festgelegten Frist abgeschlossen.

G. ZUSTÄNDIGE AUFSICHTSBEHÖRDE

Soweit die EU-DSGVO Anwendung findet, ist diejenige Aufsichtsbehörde des EU-Mitgliedstaats zuständig, in dem der Verantwortliche (oder, falls der Verantwortliche keine Niederlassung in der EU hat, sein Vertreter) niedergelassen ist. Hat der Verantwortliche weder eine Niederlassung noch einen Vertreter in der EU, ist die Irish Data Protection Commission die zuständige Aufsichtsbehörde.

Soweit die UK-DSGVO Anwendung findet, ist das UK Information Commissioner's Office die zuständige Aufsichtsbehörde.

ANHANG 2. TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN

Dieser Anhang legt die **technischen und organisatorischen Maßnahmen** (nachfolgend auch „TOM“) fest und ergänzt Abschnitt 3 des Auftragsverarbeitungsvertrags zwischen dem Auftragsverarbeiter und dem Verantwortlichen gemäß Artikel 28 der DSGVO (EU-Datenschutz-Grundverordnung Nr. 2016/679).

Informationssicherheit

Datenverschlüsselung: Verwendung von AES-256 für ruhende Daten und TLS 1.2+ für Daten während der Übertragung.
Pseudonymisierung: Verwendung von SHA-256-Hashing für anwendbare Datensätze.
Firewalls: Implementierung von Web Application Firewalls (WAF) und Firewalls auf Netzwerkebene.
Berechtigungskontrolle: Strikte Logik für den Zugriff auf Informationen auf der Grundlage von Rollen.
Resilienz: Schutz vor unbefugter Verarbeitung, Verlust oder Zerstörung.
Sicherung und Wiederherstellung: Schlüsselsysteme werden als vollständige Systemabbilder gesichert, um eine schnelle Wiederherstellung zu ermöglichen. Sicherungen werden sowohl im ruhenden Zustand als auch bei der Übertragung verschlüsselt, einschließlich Remote- und cloudbasierter Sicherungen. Sicherungs- und Wiederherstellungsverfahren werden regelmäßig getestet, um zu bestätigen, dass die Wiederherstellung voll funktionsfähig ist.
Im Falle einer Wiederherstellung aus einer Sicherung werden zuvor gelöschte personenbezogene Daten unverzüglich, in jedem Fall jedoch innerhalb von 24 Stunden nach der Wiederherstellung, aus den wiederhergestellten Daten entfernt.
DDoS-Schutz: Verwendung spezialisierter Filterdienste für Datenverkehr und automatisierter Abwehrtools, die vom Infrastrukturanbieter bereitgestellt werden, zum Schutz vor Angriffen auf die Infrastruktur (Layer 3/4) und die Anwendungsebene (Layer 7).
Patch-Management: Automatisierte Überwachung und Bereitstellung von Sicherheits-Patches für alle Cloud-Ressourcen und Betriebssysteme.

1. Vertraulichkeit

1.1. Physische Zugangskontrolle

Maßnahmen, die geeignet sind, unbefugte Personen daran zu hindern, Zugang zu Datenverarbeitungssystemen zu erhalten, mit denen personenbezogene Daten verarbeitet oder genutzt werden.

1.2. Technische Maßnahmen

Alarmanlage: Nutzung eigener fortschrittlicher Sicherheitssysteme von Ajax (Hub-Zentralen, Bewegungsmelder und Sirenen) mit 24/7-Überwachung und sofortiger Alarmierung.
Elektronische Zugangskontrolle: Sicheres System von RFID-Schlüsselkarten/Zugangsgeräten für den Bürozutritt; Zugriffsprotokolle werden geführt und regelmäßig überprüft.
Videoüberwachung: Hochauflösende IP-Kameras zur Überwachung von Ein- und Ausgangspunkten sowie internen kritischen Bereichen.
Sicherheit der Cloud-Infrastruktur: Der physische Zugang zu den Servern wird von AWS in Übereinstimmung mit seinen Konformitätszertifizierungen (SOC 2, ISO 27001) verwaltet.

1.3. Organisatorische Maßnahmen

Informationssicherheitsrichtlinie: Umfassende interne Regeln für die physische Sicherheit und den Schutz von Vermögenswerten.
Arbeitsanweisungen für Betriebssicherheit: Dokumentierte Verfahren zur Sicherung der Büroumgebung und zum Umgang mit Hardware.
Arbeitsanweisung Zugangskontrolle: Strikte Protokolle für die Erteilung, den Entzug und die

Überprüfung physischer Zugriffsrechte für Mitarbeiter und Auftragnehmer.
Richtlinie für das Besuchermanagement: Anforderungen an die Protokollierung, Identifizierung und Begleitung aller Besucher innerhalb der Büroräumlichkeiten.

2. Logische Zugangskontrolle

Maßnahmen zur Verhinderung der unbefugten Nutzung von Datenverarbeitungssystemen.

Multi-Faktor-Authentifizierung (MFA): Verpflichtend für alle administrativen Zugriffe, die Verwaltung der Cloud-Konsole und Fernanmeldungen.
Identitäts- und Zugriffsmanagement (IAM): Zentrale Verwaltung der Benutzerrechte mit regelmäßigen Zugriffsprüfungen.
VPN-Zugang: Anforderung verschlüsselter VPN-Tunnel für jede Fernverbindung zur Produktionsumgebung oder zu internen Verwaltungstools.

3. Datenzugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können.

Rollenbasierte Zugriffskontrolle (RBAC): Berechtigungen werden strikt entsprechend den spezifischen Arbeitsfunktionen und nach dem „Need-to-Know"-Prinzip vergeben.
Audit-Protokollierung: Umfassende Protokollierung aller Zugriffsaktivitäten, Änderungen und Löschungen innerhalb von Systemen, die personenbezogene Daten enthalten.

4. Integrität, Verfügbarkeit und Resilienz

Übertragungskontrolle: Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.
Eingabekontrolle: Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.
Verfügbarkeitskontrolle: Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (z. B. unterbrechungsfreie Stromversorgung (USV) in Rechenzentren, redundante Speicherung).
Betriebskontinuität und Wiederherstellung: Dokumentierte Pläne zur Aufrechterhaltung des Geschäftsbetriebs und zur Wiederherstellung im Katastrophenfall werden geführt, mindestens einmal jährlich getestet und überprüft.

5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Vorfallmanagement: Dokumentierter Prozess zur Erkennung, Meldung und Bewältigung von Sicherheitsvorfällen und potenziellen Verletzungen des Schutzes personenbezogener Daten.
Schwachstellenmanagement: Regelmäßige automatisierte Schwachstellenscans und periodische professionelle Penetrationstests der Infrastruktur und Anwendungen.
Mitarbeitersensibilisierung: Regelmäßige Schulungen für die Mitarbeiter zu den Themen Datenschutz, DSGVO-Konformität und Phishing-Bedrohungen.
Personensicherheit: Hintergrundüberprüfungen werden gemäß bewährter Einstellungspraxis durchgeführt, und alle Mitarbeiter und Auftragnehmer unterzeichnen Vertraulichkeitsvereinbarungen, bevor sie auf personenbezogene Daten zugreifen.

ANHANG 3. DIE LISTE GENEHMIGTER UNTERAUFTRAGSVERARBEITER

Die aktuelle und stets auf dem neuesten Stand befindliche Liste der vom Auftragsverarbeiter beauftragten Unterauftragsverarbeiter wird unter folgender Adresse geführt und veröffentlicht:
https://ajax.systems/gdpr-white-paper/

Der Auftragsverarbeiter aktualisiert diese Liste vor der Beauftragung eines neuen Unterauftragsverarbeiters gemäß dem in Abschnitt 7 dieses Vertrags festgelegten Verfahren.