

1 Geltungsbereich und Vertragsbestandteile

- 1.1 Diese Allgemeinen Geschäftsbedingungen («AGB») regeln den Bezug der advact Services zwischen der advact AG, Aarberggasse 20, 3011 Bern, UID CHE-341.216.036 («advact»), und ihren Kundinnen und Kunden («Kunde»). advact und der Kunde werden einzeln «Partei» und gemeinsam «Parteien» genannt.
- 1.2 Die advact Services richten sich ausschliesslich an Unternehmen, Behörden und andere Organisationen. Sie werden nicht direkt an Konsumentinnen und Konsumenten angeboten.
- 1.3 Der Vertrag zwischen den Parteien («Vertrag») besteht aus den folgenden Bestandteilen:
 - a) dem Angebot der advact, das vom Kunden angenommen wurde, inklusive allfälliger Zusatzangebote («Angebot»);
 - b) diesen AGB einschliesslich der Bestimmungen zur Auftragsbearbeitung (Ziff. 12 bis 20). Die AGB gelten mit dem Vertragsschluss, ohne dass es einer Unterzeichnung bedarf;
 - c) der «Leistungsbeschreibung advact Services» in der Fassung, die dem Angebot beiliegt («Leistungsbeschreibung»).
- 1.4 Bei Widersprüchen gilt folgende Rangfolge:
 - a) Vereinbarungen, die von beiden Parteien unterzeichnet sind und ausdrücklich auf die advact Services Bezug nehmen, einschliesslich vom Kunden gestellter Verträge, die advact unterzeichnet hat;
 - b) die Bestimmungen zur Auftragsbearbeitung (Ziff. 12 bis 20) in allen Fragen des Datenschutzes und der Datensicherheit;
 - c) das Angebot;
 - d) diese AGB;
 - e) die Leistungsbeschreibung.
- 1.5 Allgemeine Geschäfts- oder Einkaufsbedingungen des Kunden, auch solche, die in Bestellungen oder Bestellsystemen enthalten sind, gelten nicht, selbst wenn advact ihnen nicht ausdrücklich widerspricht. Sie gelten nur, soweit advact sie gemäss Ziff. 1.4 Bst. a ausdrücklich akzeptiert hat.
- 1.6 Massgebend ist die bei Vertragsschluss gültige Fassung dieser AGB. Die jeweils aktuelle Fassung ist unter www.advact.ch/agb abrufbar. Änderungen richten sich nach Ziff. 24.

2 Begriffe

- 2.1 In diesen AGB bedeuten:

- **advact Services:** das modulare Service-Portfolio der advact zur Erhöhung der E-Mail- und

Nachrichtensicherheit, bestehend aus den Modulen *Simulate* (inkl. Seasons-Strategie), *Triage*, *Extract*, *Learn* und *Insights* sowie den Portalen *Cockpit*, *Board* und *Insights*.

- **Modul:** ein im Angebot einzeln aufgeführter Baustein der advact Services. Geschuldet sind nur die im Angebot gebuchten Module.
- **Cockpit:** Portal für die Mitarbeitenden des Kunden mit ihren eigenen Resultaten und Lerninhalten (cockpit.advact.swiss).
- **Board:** Portal für die vom Kunden bezeichneten Verantwortlichen mit Auswertungen und Kennzahlen (board.advact.swiss).
- **Insights:** Portal für Kunden mit erweitertem Zugriff auf die gemeldeten verdächtigen E-Mails (*Triage*) und alle analysierten E-Mails aus *Extract*. Zusätzlich Zugriff auf Indikatorlisten der advact. Insights ist im Modul *Extract* ohne zusätzliche Lizenzkosten enthalten und kann zu *Triage* als Zusatzmodul bezogen werden.
- **advact Adminportale:** die von advact in der Schweiz entwickelte und betriebene Plattform, auf der gemeldete und als verdächtig erkannte («flagged») E-Mails (aus *Triage* und *Extract*) analysiert werden.
- **Phishing-Reporter:** das Add-in für Microsoft Outlook, mit dem User verdächtige E-Mails und Kalendereinträge an advact melden.
- **User:** die Mitarbeitenden und weiteren Personen des Kunden, für welche die advact Services gemäss Angebot bezogen werden.
- **Kundendaten:** alle Daten, die der Kunde oder seine User advact zur Verfügung stellen oder die bei der Nutzung der advact Services im Auftrag des Kunden entstehen, insbesondere Personendaten.
- **Go-Live:** der Abschluss des Onboardings, mit dem die gebuchten Module produktiv genutzt werden können. advact teilt dem Kunden das Datum des Go-Live in Textform mit.
- **Vertragsjahr:** jeweils zwölf Monate ab Beginn der Laufzeit (Ziff. 8.2), sofern das Angebot nichts anderes vorsieht.
- **Vertragsende:** das Ende der Laufzeit oder die vorzeitige Beendigung des Vertrags gemäss Ziff. 8.
- **Servicezeit:** Montag bis Freitag, 08:00 bis 17:00 Uhr, ausgenommen allgemeine Feiertage am Sitz der advact in Bern.
- **Personendaten:** alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen. Eine **betroffene Person** ist eine Person, über die Personendaten bearbeitet werden.

- **Bearbeiten:** jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, beispielsweise das Abfragen, Abgleichen, Anpassen, Archivieren, Aufbewahren, Auslesen, Bekanntgeben, Beschaffen, Erfassen, Erheben, Löschen, Offenlegen, Ordnen, Organisieren, Speichern, Verändern, Verbreiten, Verknüpfen, Vernichten und Verwenden von Personendaten.
- **Verletzung der Datensicherheit:** eine Verletzung der Sicherheit, die dazu führt, dass Personendaten unbeabsichtigt oder widerrechtlich verloren gehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden.
- **Subunternehmer:** Dritte, die advact zur Leistungserbringung bezieht; soweit sie Personendaten des Kunden bearbeiten, sind sie Unterauftragsbearbeiter im Sinne von Art. 9 Abs. 3 DSG.
- **Schriftlich:** Schriftform oder Textform, die den Nachweis durch Text ermöglicht, insbesondere E-Mail.

3 Vertragsschluss

- 3.1 Angebote der advact sind während der im Angebot genannten Gültigkeitsdauer verbindlich.
- 3.2 Der Vertrag kommt zustande, sobald der Kunde das Angebot annimmt. Als Annahme gilt, was zuerst eintritt:
 - a) die Unterzeichnung des Angebots, auch elektronisch;
 - b) eine schriftliche Annahmeerklärung, wobei eine E-Mail genügt;
 - c) eine Bestellung, die auf das Angebot Bezug nimmt;
 - d) die Inanspruchnahme der advact Services, namentlich die Mitwirkung am Onboarding (z. B. Allow-Listing, Lieferung von Userlisten, Installation des Phishing-Reporters, Erteilung von Berechtigungen für Microsoft 365), die Nutzung der Portale oder die vorbehaltlose Bezahlung der ersten Rechnung.
- 3.3 Mit der Annahme anerkennt der Kunde diese AGB sowie die Leistungsbeschreibung, die dem Angebot beiliegen oder auf die das Angebot verweist.
- 3.4 Nimmt der Kunde das Angebot nach Ablauf der Gültigkeitsdauer oder mit Änderungen an, gilt dies als neues Angebot des Kunden. Der Vertrag kommt in diesem Fall mit der schriftlichen Bestätigung der advact oder mit dem Beginn der Leistungserbringung zustande.
- 3.5 Erweiterungen, insbesondere zusätzliche Module oder User, werden mit einem Zusatzangebot vereinbart und unterstehen ebenfalls diesen AGB. Sofern das Zusatzangebot nichts anderes vorsieht, enden sie zusammen

mit dem bestehenden Vertrag und werden anteilmässig verrechnet.

4 Leistungen der advact

- 4.1 advact erbringt die im Angebot gebuchten Module gemäss Angebot und Leistungsbeschreibung. Weitere Leistungen, etwa individuelle Inhalte, Schulungen vor Ort oder Sonderauswertungen, erbringt advact nur aufgrund einer separaten Vereinbarung und gegen Vergütung.
- 4.2 advact stellt die advact Services als Software as a Service (SaaS) bereit und betreibt die dafür nötige Infrastruktur. Die Vergütung deckt insbesondere das Hosting, den Betrieb, die Wartung sowie die Verteilung von Anpassungen zur Fehlerbehebung (Updates).
- 4.3 advact entwickelt die advact Services laufend weiter und darf sie anpassen, sofern die vereinbarten wesentlichen Funktionen eines gebuchten Moduls während der Laufzeit nicht wesentlich eingeschränkt werden. Releases mit wesentlicher Funktionserweiterung sind nicht in der bisherigen Vergütung enthalten. advact unterbreitet dem Kunden dafür ein Angebot, bevor sie für ihn aktiviert werden. Über wesentliche Änderungen informiert advact den Kunden vorgängig.
- 4.4 Die Infrastruktur der advact Services befindet sich in ISO-27001-zertifizierten Rechenzentren in der Schweiz. Personendaten des Kunden werden ausschliesslich in der Schweiz gespeichert und bearbeitet (Ziff. 19).
- 4.5 Während der Servicezeit nimmt advact Störungsmeldungen entgegen und erbringt ihre Leistungen für Wartung und Pflege; sie reagiert auf Anfragen in der Regel innerhalb eines Arbeitstages. Gemeldete und als verdächtig erkannte E-Mails bearbeitet advact während der Servicezeit in der Regel innert zwei Arbeitsstunden nach Erhalt (Bearbeitungsziel); Meldungen ausserhalb der Servicezeit werden am nächsten Arbeitstag bearbeitet.
- 4.6 Als Wartungsfenster ist jeweils der letzte Samstag eines Monats zwischen 10:00 und 12:00 Uhr vorgesehen; währenddessen können die advact Services eingeschränkt sein. Dringende Sicherheitsupdates darf advact jederzeit einspielen. Eine bestimmte Verfügbarkeit ist nur geschuldet, wenn sie im Angebot ausdrücklich vereinbart ist.
- 4.7 Jede Partei kann schriftlich Änderungen der vereinbarten Leistungen beantragen. Sind Auswirkungen auf die Kosten zu erwarten, offeriert advact die Änderung. Die Änderung gilt erst, wenn die Parteien sie schriftlich vereinbart haben.

- 4.8 Teile der advact Services hängen von Produkten und Schnittstellen Dritter ab, insbesondere von Microsoft Exchange, Microsoft Outlook, Microsoft 365 und der Microsoft-Graph-API. Änderungen dieser Produkte können den Funktionsumfang beeinflussen, namentlich des Phishing-Reporters (*Triage*) und von *Extract*. advact passt die advact Services in angemessener Frist an, soweit ihr dies zumutbar ist. Für die Verfügbarkeit und Funktionsweise der Produkte Dritter übernimmt advact keine Gewähr.
- 4.9 **Keine Erfolgsgarantie: Die advact Services verringern das Risiko erfolgreicher Angriffe per E-Mail, können es aber nicht ausschliessen. advact garantiert weder ein bestimmtes Verhalten der User noch, dass *Triage* und *Extract* sämtliche schädlichen E-Mails erkennen oder ausschliesslich schädliche E-Mails entfernen.** Verdicts sind fachliche Einschätzungen nach dem Stand der Technik und dem Kenntnisstand zum Zeitpunkt der Prüfung. Die advact Services ersetzen keine eigenen Sicherheitsmassnahmen des Kunden wie Virenschutz, Datensicherung oder Notfallorganisation.
- 4.10 advact darf zur Leistungserbringung Subunternehmer beiziehen und bleibt gegenüber dem Kunden für deren Leistungen verantwortlich. Für Subunternehmer, die Personendaten des Kunden bearbeiten, gilt Ziff. 18.
- 4.11 Weder advact als Gesellschaft noch ihre Mitarbeitenden als Privatpersonen sind offen oder verdeckt wirtschaftlich an Lieferanten oder Hersteller von Hard- und Software gebunden, etwa durch Provisionen oder Beteiligungen.
- ## 5 Pflichten des Kunden
- 5.1 Der Kunde erbringt die für die Leistungserbringung nötigen Mitwirkungen rechtzeitig und unentgeltlich gemäss den Anleitungen der advact. Dazu gehören insbesondere:
- a) die Bezeichnung einer Ansprechperson sowie einer Kontaktperson für sicherheitsrelevante Eskalationen (SOC-Kontakt);
 - b) die Lieferung aktueller Userlisten, in der Regel monatlich;
 - c) das Allow-Listing auf der eigenen E-Mail- und Proxy-Infrastruktur, damit Simulationen zugestellt werden können;
 - d) die Installation des Phishing-Reporters und seine Freigabe für die User;
 - e) die Erteilung und Aufrechterhaltung der für *Extract* nötigen Berechtigungen im Microsoft-365-Tenant;
 - f) die Bezeichnung der Personen, die Zugriff auf das *Board* erhalten.
- 5.2 Erbringt der Kunde Mitwirkungen nicht oder verspätet, verschieben sich die betroffenen Termine angemessen. advact haftet nicht für die Folgen fehlender Mitwirkung. Verzögert sich der Go-Live aus Gründen, die der Kunde zu vertreten hat, um mehr als 30 Tage, darf advact die Vergütung ab diesem Zeitpunkt in Rechnung stellen.
- 5.3 Der Kunde meldet oder bestätigt advact auf Anfrage die korrekte Anzahl User. Übersteigt die tatsächliche Anzahl die vereinbarte, verrechnet advact die zusätzlichen User anteilmässig ab der Überschreitung zu den Konditionen des Angebots. Eine Reduktion ist auf das Ende eines Vertragsjahres möglich, frühestens auf das Ende der Mindestlaufzeit.
- 5.4 Der Kunde ist für die Bearbeitung der Personendaten seiner User in den advact Services datenschutzrechtlich verantwortlich. Er informiert seine Mitarbeitenden vorgängig über den Einsatz der advact Services, insbesondere über Simulationen, die Analyse gemeldeter und eingehender E-Mails, die Seasons-Strategie und personenbezogene Auswertungen. Er wahrt allfällige Mitwirkungsrechte der Personalvertretung und beachtet die arbeitsrechtlichen Vorgaben, namentlich Art. 328b OR und Art. 26 der Verordnung 3 zum Arbeitsgesetz (ArGV 3). Soweit erforderlich, führt er eine Datenschutz-Folgenabschätzung durch.
- 5.5 Benutzerkonten sind persönlich. Der Kunde hält Zugangsdaten geheim, nutzt die angebotene Mehr-Faktor-Authentifizierung (MFA) und meldet advact unverzüglich jeden Verdacht auf Missbrauch. Er ist für Handlungen verantwortlich, die über seine Zugänge erfolgen.
- 5.6 Stellt der Kunde Inhalte oder Kennzeichen zur Verfügung, etwa Logos, Weisungen, Beispiele, eigene Lerninhalte oder Vorgaben für Simulationen, sichert er zu, dass er dazu berechtigt ist und die Inhalte rechtmässig sind. Er räumt advact das unentgeltliche, nicht ausschliessliche Recht ein, diese Inhalte während der Laufzeit für die Leistungserbringung zu verwenden.
- 5.7 Simulationen ahmen realistische Absender und Kennzeichen Dritter nach, beispielsweise von Logistik-, Finanz- oder Softwareunternehmen. Sie dienen ausschliesslich der Sensibilisierung innerhalb der Organisation des Kunden. Der Kunde kann bestimmte Absender, Marken oder Themen ausschliessen. Er informiert seine IT-Dienstleister, die von Simulationen betroffen sein könnten, vorgängig, insbesondere externe Betreiber eines Security Operations Centers (SOC).
- 5.8 Dem Kunden ist insbesondere untersagt:
- a) den Phishing-Reporter einschliesslich aller Bestandteile an Dritte weiterzugeben, zu kopieren

- oder für zusätzliche, nicht vereinbarte User zu nutzen;
- b) Dritten Zugang zu den advact Services zu verschaffen, ausgenommen vom Kunden beauftragte Dritte wie ein externes SOC, für die der Kunde einsteht;
- c) die Software zu dekompile, zurückzuentwickeln oder zu verändern, soweit dies nicht zwingend gesetzlich erlaubt ist;
- d) Sicherheits- oder Lasttests an den advact Services ohne vorgängige schriftliche Zustimmung der advact durchzuführen, vorbehältlich des Bug-Bounty-Programms der advact (www.advact.ch/advact/bug-bounty-program-policy);
- e) die advact Services für rechtswidrige Zwecke oder für Simulationen gegenüber Personen ausserhalb der eigenen Organisation zu verwenden;
- f) Regeln, Listen und Indikatoren der advact zu vermarkten, an Dritte weiterzugeben oder damit ein Konkurrenzprodukt zu entwickeln.
- 5.9 Der Kunde ist selbst dafür verantwortlich, die Lizenzvorschriften aller Software, Software-Werkzeuge und Betriebssysteme einzuhalten, die er direkt einsetzt.
- ## 6 Nutzungsrechte und Schutzrechte
- 6.1 advact räumt dem Kunden für die Laufzeit das nicht ausschliessliche, nicht übertragbare und nicht unterlizenzierbare Recht ein, die gebuchten Module für interne Zwecke und für die vereinbarte Anzahl User zu nutzen. Das Nutzungsrecht setzt die fristgerechte Bezahlung der Vergütung voraus.
- 6.2 Für den Phishing-Reporter umfasst das Nutzungsrecht die Installation in der Umgebung des Kunden für die vereinbarten User. Nach Vertragsende entfernt der Kunde den Phishing-Reporter.
- 6.3 Mit *Insights* darf der Kunde die Regeln, Listen und Indikatoren der advact während der Laufzeit in seinen eigenen Sicherheitssystemen für interne Schutzzwecke verwenden. Indikatoren, die bis zum Vertragsende in seine Systeme übernommen wurden, darf er danach weiter für interne Schutzzwecke verwenden.
- 6.4 Alle Rechte an der Software, den Portalen, den Simulationsvorlagen, den Lernmodulen, den Regeln und Listen sowie an der Dokumentation bleiben bei advact oder ihren Lizenzgebern. Schutzrechte, die bei der Vertragserfüllung entstehen, namentlich Urheber-, Patent-, Design- oder Markenrechte, stehen ausschliesslich advact zu, soweit nichts anderes vereinbart ist. Alle Rechte, die dem Kunden nicht ausdrücklich eingeräumt werden, bleiben vorbehalten.
- 6.5 Die Kundendaten verbleiben beim Kunden. advact bearbeitet sie ausschliesslich zur Vertragserfüllung gemäss Ziff. 12 bis 20, vorbehältlich Ziff. 6.6.
- 6.6 **Threat Intelligence und anonymisierte Daten: Der Kunde nimmt zur Kenntnis und ist einverstanden, dass advact die Randdaten gemeldeter und als verdächtig erkannter E-Mails sowie die daraus gewonnenen technischen Indikatoren (z. B. Domains, URLs, Hashes, Muster) in eigener Verantwortung zur Erkennung und Abwehr von Cyberangriffen verwendet, auch zum Schutz anderer Kunden.** Inhalte von E-Mails und Angaben, die Rückschlüsse auf den Kunden zulassen, gibt advact nicht an andere Kunden weiter. advact darf zudem anonymisierte und aggregierte Statistiken erstellen und verwenden, etwa Klick- und Meldequoten nach Branche. Einzelheiten regelt Ziff. 14.
- 6.7 Anregungen und Rückmeldungen des Kunden zu den advact Services darf advact unentgeltlich für deren Weiterentwicklung verwenden.
- ## 7 Vergütung und Zahlungsbedingungen
- 7.1 Für die advact Services schuldet der Kunde die im Angebot festgelegte, volumenabhängige Vergütung zu einem Fixpreis pro User. Alle Preise verstehen sich in Schweizer Franken und zuzüglich der gesetzlichen Mehrwertsteuer.
- 7.2 Sofern das Angebot nichts anderes vorsieht, stellt advact die Vergütung jährlich im Voraus in Rechnung. Die Verrechnung beginnt mit dem im Angebot genannten Leistungsbeginn, ohne solche Angabe mit dem Go-Live.
- 7.3 Zusätzliche User und Module stellt advact direkt nach deren Vereinbarung anteilmässig in Rechnung.
- 7.4 advact kann die Preise auf den Beginn eines neuen Vertragsjahres nach Ablauf der Mindestlaufzeit anpassen. Sie teilt Preisanpassungen mindestens zwei Monate vor Ablauf des laufenden Vertragsjahres schriftlich mit. Der Kunde kann den Vertrag in diesem Fall auf das Inkrafttreten der neuen Preise gemäss Ziff. 8 kündigen.
- 7.5 Rabatte, die an eine Laufzeit oder an eine Anzahl Module geknüpft sind, gelten nur, solange ihre Voraussetzungen erfüllt sind.
- 7.6 Rechnungen sind innerhalb von 30 Tagen nach Rechnungsdatum ohne Abzug zur Zahlung fällig. Mit unbenutztem Ablauf der Zahlungsfrist kommt der Kunde automatisch in Verzug, ohne dass es einer Mahnung bedarf. Ab Verzug schuldet der Kunde einen Verzugszins von acht Prozent (8 %) pro Jahr.
- 7.7 Einwände gegen Rechnungen müssen innerhalb von 15 Tagen nach Rechnungsdatum schriftlich und begründet bei advact eingehen. Andernfalls gilt die Rechnung als

genehmigt. Unbestrittene Teile einer Rechnung sind fristgerecht zu bezahlen.

- 7.8 Der Kunde darf nur mit Forderungen verrechnen, die advact anerkannt hat oder die rechtskräftig festgestellt sind.
- 7.9 Ist der Kunde trotz Mahnung mit einer Nachfrist von zehn Tagen weiterhin in Verzug, darf advact den Zugang zu den advact Services nach vorgängiger Ankündigung sperren. Die Pflicht zur Zahlung der Vergütung bleibt bestehen. Solange der Kunde mit fälligen Zahlungen im Verzug ist, darf advact zudem die Mängelbehebung verweigern.

8 Laufzeit und Beendigung

- 8.1 Der Vertrag tritt mit dem Vertragsschluss gemäss Ziff. 3 in Kraft.
- 8.2 Die Laufzeit beginnt mit dem im Angebot genannten Leistungsbeginn, ohne solche Angabe mit dem Go-Live. Die Mindestlaufzeit richtet sich nach dem Angebot und beträgt mindestens ein Jahr (365 Tage).
- 8.3 Nach Ablauf der Mindestlaufzeit verlängert sich der Vertrag jeweils um ein Jahr, sofern ihn keine Partei unter Einhaltung einer Kündigungsfrist von einem Monat auf das Ende der Mindestlaufzeit oder eines Vertragsjahres schriftlich kündigt. Die Kündigung kann sich auf einzelne Module beschränken.
- 8.4 Jede Partei kann den Vertrag oder einzelne Module aus wichtigem Grund jederzeit schriftlich mit sofortiger Wirkung kündigen. Ein wichtiger Grund liegt insbesondere vor:
- a) bei einer wesentlichen Vertragsverletzung der anderen Partei, die trotz schriftlicher Abmahnung nicht innerhalb von 30 Tagen behoben wird;
 - b) wenn über die andere Partei der Konkurs eröffnet oder ihr eine Nachlassstundung gewährt wird;
 - c) in den Fällen gemäss Ziff. 9.4 (Mängel), Ziff. 24.3 (Änderung der AGB) und Ziff. 18.2 (Widerspruch gegen Subunternehmer).
- 8.5 Mit der Beendigung enden die Nutzungsrechte und advact sperrt die Zugänge. Der Kunde entfernt den Phishing-Reporter und entzieht die für Extract erteilten Berechtigungen. Bis zum Vertragsende kann der Kunde Auswertungen aus dem Board exportieren. Die Rückgabe und Löschung von Personendaten richten sich nach Ziff. 15.7 bis 15.9.
- 8.6 Im Voraus bezahlte Vergütungen werden nicht zurück-erstattet. Kündigt der Kunde aus einem wichtigen Grund, den advact zu vertreten hat, oder gemäss Ziff. 24.3 oder Ziff. 18.2, erstattet advact die bereits bezahlte Vergütung für die Zeit nach der Beendigung anteilmässig zurück.

9 Gewährleistung

- 9.1 advact gewährleistet, dass die advact Services bei vertragsgemäsem Einsatz die ausdrücklich zugesicherten Eigenschaften aufweisen und nicht mit Mängeln behaftet sind, die ihre Tauglichkeit aufheben oder erheblich einschränken. Als zugesichert gelten nur Eigenschaften, die im Angebot ausdrücklich als zugesichert bezeichnet sind.
- 9.2 advact gewährleistet, dass der Kunde Zugriff auf das Board (board.advact.swiss) erhält, auf den Auswertungen zu den advact Services angeboten werden.
- 9.3 advact gewährleistet, dass der Phishing-Reporter in den von Microsoft unterstützten Versionen von Microsoft Exchange und Microsoft 365 hinzugefügt werden kann und in Standardinstallationen der von Microsoft unterstützten Versionen von Microsoft Outlook (Windows, Mac, neues Outlook sowie Outlook im Web in unterstützten Browsern) funktioniert, solange Microsoft diese Versionen unterstützt. Die aktuelle Liste der getesteten Versionen stellt advact auf Anfrage zur Verfügung.
- 9.4 Der Kunde meldet Mängel unverzüglich und nachvollziehbar dokumentiert. advact behebt Mängel innert angemessener Frist durch Nachbesserung oder eine zumutbare Umgehungslösung. Schlagen zwei Nachbesserungsversuche wegen desselben Mangels fehl, kann der Kunde nach seiner Wahl eine Minderung verlangen oder das betroffene Modul aus wichtigem Grund kündigen. Die Minderung ist auf 25 % der Vergütung des betroffenen Moduls für die Dauer des Mangels begrenzt.
- 9.5 advact haftet nicht für Mängel, die auf Produkten oder Diensten von Microsoft oder anderer Dritter, auf der Infrastruktur des Kunden, auf unsachgemässer Nutzung oder auf fehlender Mitwirkung des Kunden beruhen.
- 9.6 Jede weitere Gewährleistung, namentlich für bestimmte Erkennungs-, Klick- oder Meldequoten, ist ausgeschlossen, soweit gesetzlich zulässig.

10 Haftung

- 10.1 advact haftet unbeschränkt für absichtlich oder grobfahrlässig verursachte Schäden, für Personenschäden sowie nach zwingenden gesetzlichen Bestimmungen, etwa dem Produkthaftungsgesetz (Art. 100 Abs. 1 OR).
- 10.2 Im Übrigen ist die Haftung der advact für Schäden aus oder im Zusammenhang mit dem Vertrag insgesamt auf den Betrag der Vergütung begrenzt, die der Kunde für das Vertragsjahr bezahlt hat, in dem das schädigende Ereignis eingetreten ist.
- 10.3 Soweit gesetzlich zulässig, ist die Haftung für indirekte Schäden und Folgeschäden ausgeschlossen,

insbesondere für entgangenen Gewinn, nicht realisierte Einsparungen, Datenverlust, Reputationsschäden und Ansprüche Dritter.

10.4 Soweit gesetzlich zulässig, haftet advact insbesondere nicht für:

- a) Viren oder andere Schadsoftware in der IT-Umgebung des Kunden, namentlich solche, die mit dem Phishing-Reporter weitergeleitet wurden;
- b) Schäden, die entstehen, während der Phishing-Reporter oder *Triage* nicht funktioniert oder ausgeschaltet ist;
- c) Schäden aus Verdicts, aus nicht erkannten schädlichen E-Mails oder aus der Entfernung legitimer E-Mails durch *Extract*;
- d) Ausfälle, Störungen und Änderungen von Produkten und Diensten von Microsoft oder anderer Dritter;
- e) Massnahmen, die der Kunde gestützt auf Auswertungen gegenüber seinen Mitarbeitenden trifft;
- f) die gesetzeskonforme Meldung von Funden gemäss Ziff. 21.

10.5 Für beigezogene Dritte, namentlich Subunternehmer, haftet advact im gleichen Umfang wie für eigenes Verhalten. Die Haftungsbeschränkungen dieser Ziff. 10 gelten auch zugunsten der Mitarbeitenden und der beigezogenen Dritten.

10.6 Im Verhältnis zwischen den Parteien ist der Kunde als Verantwortlicher für die Rechtmässigkeit der Bearbeitung von Personendaten verantwortlich; advact haftet für die Einhaltung ihrer Pflichten als Auftragsbearbeiterin. Die Haftungsbeschränkungen dieser Ziff. 10 gelten auch für Ansprüche aus den Ziffern 12 bis 20. Vorbehalten bleiben zwingende gesetzliche Ansprüche betroffener Personen.

10.7 Der Kunde haftet für die Verletzung seiner Pflichten gemäss Ziff. 5. Er stellt advact von Ansprüchen Dritter, einschliesslich seiner Mitarbeitenden und Behörden, frei, die auf von ihm gelieferten Inhalten, auf einer fehlenden Information seiner Mitarbeitenden oder auf einer fehlenden Rechtsgrundlage für die Bearbeitung beruhen.

11 Vertraulichkeit

11.1 Die Parteien behandeln alle nicht allgemein bekannten Informationen der anderen Partei vertraulich, von denen sie im Zusammenhang mit dem Vertrag Kenntnis erhalten, insbesondere Geschäftsgeheimnisse, sicherheitsrelevante Informationen, Kundendaten, Prüfberichte und die Vertragskonditionen. Sie verwenden diese Informationen nur zur Vertragserfüllung und schützen sie

mindestens mit der Sorgfalt, die sie für eigene vertrauliche Informationen anwenden.

11.2 Die Pflicht gilt nicht für Informationen, die allgemein bekannt sind oder werden, ohne dass die empfangende Partei dies zu vertreten hat, die ihr bereits rechtmässig bekannt waren, die sie unabhängig entwickelt hat oder die sie aufgrund einer gesetzlichen oder behördlichen Pflicht offenlegen muss. Im letzten Fall informiert sie die andere Partei vorgängig, soweit dies zulässig ist.

11.3 advact verpflichtet ihre Mitarbeitenden sowie allfällig beigezogene Dritte, sämtliche Informationen, die sie über den Kunden und dessen bearbeitete Daten erhalten, vertraulich zu behandeln. Diese Pflicht gilt auch nach dem Ende ihrer Tätigkeit für advact.

11.4 Untersteht der Kunde einem Berufs-, Amts- oder Bankgeheimnis, etwa nach Art. 320 oder Art. 321 StGB oder nach Art. 47 des Bankengesetzes, wahrt advact dieses Geheimnis als vom Kunden beigezogene Dritte. advact weist ihre Mitarbeitenden auf die strafrechtlichen Folgen einer Verletzung hin, einschliesslich Art. 62 DSG. Bearbeitet der Kunde klassifizierte Informationen oder hat er besondere Geheimhaltungsanforderungen, teilt er dies advact vor Vertragsschluss mit; die Parteien regeln dies gesondert.

11.5 advact unterzeichnet auf Wunsch des Kunden zusätzlich eine Geheimhaltungsvereinbarung. advact empfiehlt dem Kunden, die Vertraulichkeit auch mit seinen eigenen Mitarbeitenden schriftlich zu regeln.

11.6 Die Vertraulichkeitspflicht gilt während der Laufzeit und während fünf Jahren nach dem Vertragsende. Für Kundendaten und Geschäftsgeheimnisse gilt sie zeitlich unbeschränkt.

11.7 advact nennt den Kunden nur mit dessen vorgängiger schriftlicher Zustimmung als Referenz.

12 Datenschutz: Grundsätze und Rollen

12.1 Bei der Bearbeitung von Personendaten in den advact Services ist der Kunde der Verantwortliche und advact die Auftragsbearbeiterin. **Die Ziffern 12 bis 20 bilden die Auftragsbearbeitungsvereinbarung der Parteien.** Sie gelten mit dem Vertragsschluss ohne Unterzeichnung, nur für die gebuchten Module und für die Laufzeit des Vertrags sowie darüber hinaus, bis advact alle Personendaten des Kunden gelöscht oder zurückgegeben hat. Sie erfüllen die Anforderungen von Art. 9 DSG sowie – soweit anwendbar – von Art. 28 DSGVO.

12.2 Die Parteien bearbeiten Personendaten im Einklang mit dem schweizerischen Datenschutzrecht, insbesondere dem Bundesgesetz über den Datenschutz (DSG) und der Datenschutzverordnung (DSV). Untersteht der Kunde für die Bearbeitung einem kantonalen

Datenschutzgesetz oder der Datenschutz-Grundverordnung der EU (DSGVO), gelten deren Anforderungen an die Auftragsbearbeitung ergänzend. Für Kunden, die der DSGVO unterstehen, gelten die Ziffern 12 bis 20 zugleich als Vertrag nach Art. 28 DSGVO; die Begriffe sind entsprechend auszulegen (z. B. «Bearbeitung» als «Verarbeitung», «Auftragsbearbeiterin» als «Auftragsverarbeiter»).

- 12.3 Haben die Parteien eine eigene, von beiden unterzeichnete Auftragsbearbeitungsvereinbarung abgeschlossen, geht diese den Ziffern 12 bis 20 vor.
- 12.4 advact bearbeitet die Personendaten ausschliesslich im Auftrag und nach den dokumentierten Weisungen des Kunden. Als Weisungen gelten der Vertrag, die Einstellungen des Kunden in den Portalen sowie schriftliche Einzelweisungen des Kunden.
- 12.5 Ist advact der Ansicht, dass eine Weisung gegen Datenschutzrecht verstösst, informiert sie den Kunden unverzüglich. Sie darf die Ausführung der Weisung aussetzen, bis der Kunde sie bestätigt oder ändert. Einzelweisungen, die über den vereinbarten Leistungsumfang hinausgehen, führt advact gegen Vergütung des Aufwands aus.
- 12.6 Ansprechstelle für den Datenschutz bei advact: advact AG, Aarberggasse 20, 3011 Bern, compliance@advact.ch.
- 12.7 Für eigene Bearbeitungen ist advact selbst verantwortlich, namentlich für die Vertragsabwicklung, die Kontaktdaten der Ansprechpersonen des Kunden, den Betrieb und die Sicherheit ihrer Systeme sowie die Threat Intelligence gemäss Ziff. 6.6 und 14. Darüber informiert die «Datenschutzerklärung (DSE) advact Services», die advact dem Kunden mit dem Angebot abgibt und auf Anfrage zur Verfügung stellt.

13 Art, Umfang und Zweck der Bearbeitung

- 13.1 advact bearbeitet nur jene Personendaten und nur zu jenen Zwecken, die zur Erbringung der gebuchten Module erforderlich sind: Sensibilisierung der User, Analyse und Abwehr von Bedrohungen per E-Mail sowie Auswertungen für den Kunden.
- 13.2 Betroffene Personen sind die Mitarbeitenden und weiteren User des Kunden sowie Dritte, deren Personendaten in gemeldeten oder analysierten E-Mails enthalten sind, insbesondere Absender und Empfänger.
- 13.3 Je Modul bearbeitet advact die folgenden Personendaten:

Simulate (inkl. Seasons)

Personendaten und Bearbeitung: E-Mail-Adresse, Vor- und Nachname, Telefonnummer, Sprache. Je nach Kunde zusätzlich Angaben, die er für gewünschte

Auswertungen liefert, z. B. Geschlecht, Kaderstufe, Abteilung, Standort, Dienstalter oder Alter.

Verhalten in Simulationen (z. B. Klicks, Dateneingaben, Meldungen) sowie Browser- und Gerätedaten bei Fehlverhalten in einer Simulation.

Seasons: Punktestand, Tier, Shields und Awareness Score pro Person.

Aufbewahrung: Vertragsdauer; Löschung spätestens 30 Tage nach Vertragsende.

Ausgetretene Mitarbeitende (nicht mehr auf der Userliste) werden automatisch inaktiv gesetzt und nach 6 Monaten Inaktivität unwiderruflich anonymisiert (E-Mail-Adresse, Vor- und Nachname).

Triage

Personendaten und Bearbeitung: E-Mail-Adresse der meldenden Person, Outlook-Version und -Sprache.

Die gemeldete E-Mail bzw. der gemeldete Kalendereintrag vollständig als .eml-Datei (Header, Inhalt, Anhänge). Darin können Personendaten unterschiedlichster Kategorien enthalten sein.

Verdict und Bearbeitung durch Analysten der advact. Speicherung im advact Adminportal und im Board.

Aufbewahrung: Inhalte max. 30 Tage, als gefährlich gekennzeichnete E-Mails max. 90 Tage, vertrauliche E-Mails sofort nach der Bearbeitung (Ziff. 15).

Randdaten gemäss Ziff. 14.

Extract

Personendaten und Bearbeitung: Sämtliche eingehenden E-Mails der vom Kunden für *Extract* freigeschalteten Mailboxen werden über die Microsoft-Graph-API abgerufen und auf der Infrastruktur der advact in der Schweiz automatisch analysiert, in erster Linie durch Software.

Schlägt eine Regel an («flagged»), wird die E-Mail an das advact Adminportal übermittelt und dort von einer Analystin oder einem Analysten geprüft. Flagged und zusätzlich gemeldete E-Mails werden im Board gespeichert.

Aufbewahrung: Nicht geflaggte E-Mails werden nicht gespeichert («cleared»). Flagged E-Mails wie *Triage*.

Insights

Personendaten und Bearbeitung: Gemeldete E-Mails samt Header, Inhalt, Anhängen und Verdict; Bereitstellung über die Weboberfläche, eine API und SIEM-Webhooks an die vom Kunden bestimmten Systeme. Flagged E-Mails wie *Triage*.

Zugriff über Insights auf alle E-Mails des Kunden (*Extract*) möglich. Der User muss den Zugriff anfordern und begründen. Dies wird in einem unveränderbaren Audit Log aufgezeichnet.

Aufbewahrung: Bei advact wie *Triage*. In den Systemen des Kunden: Verantwortung des Kunden (Ziff. 15.5).

Learn

Personendaten und Bearbeitung: Name, E-Mail-Adresse und Sprache; zugewiesene und abgeschlossene Lernmodule, Lernfortschritt; bei Pflichtschulungen auf Wunsch des Kunden Erinnerungen und Abschlussnachweise.

Aufbewahrung: Vertragsdauer; Löschung spätestens 30 Tage nach Vertragsende.

Cockpit und Board

Personendaten und Bearbeitung: *Cockpit:* ausschliesslich eigene Daten der Mitarbeitenden (z. B. Tier, Shields, Lernfortschritt).

Board: Auswertungen wie Klick- und Meldequoten, Trends und Risikobereiche bis auf Stufe Abteilung oder Standort sowie Exporte (XLSX, CSV, teils PNG); Benutzerkonten und Rollen der *Board*-Benutzerinnen und -Benutzer.

Aufbewahrung: Abgeleitet aus den Modulen; Benutzerkonten bis 30 Tage nach Vertragsende.

- 13.4 Der Kunde legt fest, wer Zugriff auf das *Board* erhält. Auswertungen im *Board* sind standardmässig pseudonymisiert voreingestellt; auf Wunsch des Kunden richtet advact sie mit Personenbezug ein. Für exportierte Daten ist der Kunde verantwortlich.
- 13.5 Der Kunde liefert nur jene Angaben über seine Mitarbeitenden, die er für die gewünschten Auswertungen benötigt.
- 13.6 Die Messung des Verhaltens in Simulationen kann ein Profiling im Sinne von Art. 5 lit. f DSG darstellen. Ob und wie der Kunde Ergebnisse einzelnen Mitarbeitenden zuordnet und verwendet, entscheidet er als Verantwortlicher. advact empfiehlt, die Ergebnisse ausschliesslich zur Sensibilisierung zu verwenden.
- 13.7 Gemeldete und analysierte E-Mails können besonders schützenswerte Personendaten enthalten. advact sucht nicht gezielt danach und behandelt erkennbar vertrauliche E-Mails gemäss Ziff. 15.4. Der Kunde weist seine Mitarbeitenden darauf hin, keine privaten oder offensichtlich vertraulichen E-Mails zu melden.

14 Threat Intelligence: Bearbeitung in eigener Verantwortung der advact

- 14.1 Die Randdaten aller als verdächtig gemeldeten und aller flagged E-Mails, die nach Ziff. 15.2 länger aufbewahrten E-Mails sowie die daraus gewonnenen Indikatoren (z. B. Domains, URLs, Hashes, Muster) nutzt advact zur Erkennung und Abwehr von Cyberangriffen, auch zum Schutz anderer Kunden. Als Randdaten gelten Absender, Empfänger, meldende Person (Reporter), Betreff, Datum und Verdict.

- 14.2 Für diese Bearbeitung ist advact selbst verantwortlich. Sie stützt sich auf ihr überwiegendes berechtigtes Interesse an der Informationssicherheit ihrer Kunden (Art. 31 Abs. 1 DSG; Art. 6 Abs. 1 lit. f DSGVO). Die Randdaten werden bis zu 5 Jahre aufbewahrt.

- 14.3 Der Kunde ist mit dieser Bekanntgabe einverstanden und informiert seine Mitarbeitenden darüber, advact stellt ihm dafür die «Datenschutzerklärung (DSE) advact Services» zur Verfügung. Inhalte von E-Mails und Angaben, die Rückschlüsse auf den Kunden zulassen, gibt advact nicht an andere Kunden weiter.

- 14.4 Betroffene Personen können ihre Rechte insoweit direkt bei advact geltend machen (compliance@advact.ch).

15 Aufbewahrung und Löschung

- 15.1 Die Inhalte der als verdächtig gemeldeten und der flagged E-Mails werden grundsätzlich maximal 30 Tage im advact Adminportal und im *Board* aufbewahrt und danach automatisch gelöscht.
- 15.2 Einzelne klar als «gefährlich» erkennbare E-Mails können Analysten zur vertieften Analyse von Mustern und Angriffsarten für längstens 90 Tage zur Aufbewahrung kennzeichnen.
- 15.3 Gemeldete und flagged E-Mails werden während der Servicezeit in der Regel innert zwei Arbeitsstunden nach Erhalt bearbeitet (Bearbeitungsziel gemäss Ziff. 4.5).
- 15.4 Erhält advact E-Mails mit offensichtlich vertraulichem Inhalt oder mit offensichtlich echten Personendaten, beantworten die Analysten sie mit dem Verdict «confidential». Die meldende Person erhält die Rückmeldung, dass die E-Mail harmlos war. Der Inhalt der E-Mail wird nach der Bearbeitung **sofort automatisch** gelöscht; aufbewahrt werden nur die Randdaten ohne Inhalt und Anhänge. Auf Wunsch des Kunden wird zusätzlich automatisch eine Stelle beim Kunden, etwa die Datenschutzstelle, informiert.
- 15.5 Hat advact eine E-Mail mit vertraulichem Inhalt über *Insights* bereits an Systeme des Kunden übermittelt, bevor sie gelöscht wurde, ist der Kunde für die Löschung in seinen Systemen verantwortlich.
- 15.6 In verschlüsselten, unveränderbaren Sicherungskopien in der Schweiz können Daten bis zu ihrer ordentlichen Überschreibung, längstens 12 Monate, vorhanden sein. Auf Sicherungskopien wird nur zur Wiederherstellung zugegriffen; wiederhergestellte Daten werden erneut nach dieser Ziffer gelöscht.
- 15.7 Nach Vertragsende löscht advact die im Auftrag des Kunden bearbeiteten Personendaten innert der Fristen gemäss Ziff. 13 und 15, spätestens 30 Tage nach Vertragsende, sofern der Kunde nicht vorher schriftlich die

Herausgabe der Daten in einem gängigen Format oder eine Verlängerung der Frist verlangt. Vorbehalten bleiben gesetzliche Aufbewahrungspflichten (Ziff. 15.8).

15.8 Ausgenommen sind Daten, die advact gemäss Ziff. 14 in eigener Verantwortung bearbeitet, anonymisierte Daten, Sicherungskopien bis zu ihrer ordentlichen Überschreibung (Ziff. 15.6) sowie Daten, die advact aufgrund gesetzlicher Pflichten aufbewahren muss.

15.9 Auf Wunsch bestätigt advact dem Kunden die Löschung schriftlich.

16 Informationssicherheit und Pflichten der advact

16.1 advact trifft angemessene technische und organisatorische Massnahmen (TOM), um die Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit der Kundendaten zu schützen. Sie überprüft sie regelmässig und passt sie dem Risiko und dem Stand der Technik an. advact lässt die Massnahmen jährlich durch eine unabhängige Prüfgesellschaft in einem ISAE-3000-Typ-2-Bericht beurteilen. Eine Beschreibung der TOM und den jeweils aktuellen Bericht erhält der Kunde auf Anfrage und unter Wahrung der Vertraulichkeit.

16.2 advact darf die Massnahmen weiterentwickeln, sofern das Schutzniveau nicht unterschritten wird. Wesentliche Änderungen teilt advact den Kunden zeitnah mit.

16.3 advact verpflichtet alle Personen, die Zugang zu Personendaten des Kunden haben, zur Vertraulichkeit. Diese Pflicht gilt auch nach dem Ende ihrer Tätigkeit.

16.4 Soweit advact als Auftragsbearbeiterin handelt, ist der Kunde für die Beantwortung von Anfragen betroffener Personen zuständig. advact leitet solche Anfragen unverzüglich, spätestens innert fünf Arbeitstagen, an den Kunden weiter, beantwortet sie nur auf seine Weisung und unterstützt ihn mit geeigneten technischen und organisatorischen Massnahmen.

16.5 advact unterstützt den Kunden bei Datenschutz-Folgenabschätzungen, bei vorgängigen Konsultationen des EDÖB oder der zuständigen Aufsichtsbehörde sowie bei der Erfüllung seiner Melde- und Informationspflichten. Aufwand, der über den üblichen Rahmen hinausgeht, wird angemessen vergütet, sofern die Ursache nicht bei advact liegt.

16.6 Verlangt eine Behörde die Herausgabe von Personendaten des Kunden, informiert advact den Kunden vorgängig, soweit dies zulässig ist, und gibt Daten nur heraus, wenn sie rechtlich dazu verpflichtet ist.

17 Verletzungen der Datensicherheit

17.1 advact meldet dem Kunden Verletzungen der Datensicherheit, die Personendaten aus den advact Services betreffen, so rasch als möglich, spätestens innert 24 Stunden nach Kenntnisnahme.

17.2 Die Meldung enthält, soweit bekannt, die Art und den Zeitpunkt der Verletzung, die betroffenen Kategorien und die ungefähre Anzahl betroffener Personen und Daten, die möglichen Folgen sowie die ergriffenen oder vorgesehenen Massnahmen. advact ergänzt die Meldung, sobald weitere Informationen vorliegen.

17.3 advact unterstützt den Kunden bei der Meldung an den EDÖB bzw. an die zuständige Aufsichtsbehörde und bei der Information der betroffenen Personen.

18 Subunternehmer

18.1 Der Kunde genehmigt mit dem Vertragsschluss die Subunternehmer, die in der «Datenschutzerklärung (DSE) advact Services» aufgeführt sind, die er mit dem Angebot erhält. Er erteilt advact zudem die allgemeine Genehmigung, weitere Subunternehmer nach Ziff. 18.2 beizuziehen oder bestehende zu ersetzen.

18.2 advact informiert den Kunden mindestens 30 Tage im Voraus schriftlich über jeden neuen oder ersetzten Subunternehmer. Der Kunde kann innert dieser Frist aus wichtigen datenschutzrechtlichen Gründen schriftlich widersprechen. Die Parteien suchen in diesem Fall nach einer Lösung. Finden sie keine, kann der Kunde die betroffenen Module auf den Zeitpunkt des Bezugs kündigen. Widerspricht der Kunde nicht, gilt der Subunternehmer als genehmigt.

18.3 advact verpflichtet ihre Subunternehmer vertraglich zu einem gleichwertigen Datenschutz und bleibt gegenüber dem Kunden für sie verantwortlich.

18.4 Nicht als Subunternehmer im Sinne dieser AGB gelten Dritte, die Nebenleistungen ohne Zugriff auf Personendaten des Kunden erbringen, etwa Telekommunikations-, Post- oder Transportdienste, Hardware-Wartung ohne Datenzugriff oder die Entsorgung von Datenträgern mit Vernichtungsnachweis.

19 Bearbeitungsort

19.1 Die Personendaten werden ausschliesslich in der Schweiz gespeichert und bearbeitet. Den Mitarbeitenden der advact ist der Zugriff auf Personendaten von ausserhalb der Schweiz untersagt; er ist technisch unterbunden.

19.2 Ausgenommen ist die Übermittlung über *Insights* an die vom Kunden bestimmten Systeme; für deren Standort ist der Kunde verantwortlich. Zur Prüfung auf Schadhafteit kann advact zudem technische Merkmale wie URLs aus E-Mails externer Absender, etwa URLs oder Root-Domains, an externe Analyse- und Reputationsdienste übermitteln. Dabei werden keine Personendaten übermittelt. Diese Dienste können sich ausserhalb der Schweiz befinden. Weitere Inhalte von E-Mails verlassen die Infrastruktur der advact nicht.

19.3 Eine Bekanntgabe von Personendaten ins Ausland erfolgt nur, wenn die Voraussetzungen von Art. 16 f. DSGVO und – soweit anwendbar – von Kapitel V DSGVO erfüllt sind. Die Übermittlung von Personendaten aus der EU in die Schweiz stützt sich auf den Angemessenheitsbeschluss der Europäischen Kommission für die Schweiz.

20 Nachweise, Kontrollen und Protokollierung

20.1 advact stellt dem Kunden die Informationen zur Verfügung, die zum Nachweis der Einhaltung der Ziffern 12 bis 20 erforderlich sind.

20.2 advact lässt jährlich einen ISAE-3000-Typ-2-Bericht durch eine unabhängige Prüfgesellschaft (derzeit BDO) erstellen. Der Kunde kann den jeweils aktuellen Bericht unter Wahrung der Vertraulichkeit anfordern.

20.3 Der Kunde hat das Recht, nach Absprache mit advact Überprüfungen selbst durchzuführen oder durch im Einzelfall zu benennende, zur Verschwiegenheit verpflichtete unabhängige Prüfer durchführen zu lassen, die keine Wettbewerber der advact sind. Er kann sich durch Stichprobenkontrollen, die in der Regel 30 Tage im Voraus anzumelden sind, während der Geschäftszeiten von der Einhaltung der Ziffern 12 bis 20 überzeugen. Ohne besonderen Anlass, etwa eine Verletzung der Datensicherheit, finden Kontrollen höchstens einmal pro Jahr statt.

20.4 Kontrollen dürfen die Vertraulichkeit gegenüber anderen Kunden und die Sicherheit der advact Services nicht gefährden. Der Kunde trägt die Kosten der Kontrolle, es sei denn, sie deckt einen wesentlichen Verstoß der advact auf.

20.5 Die Prüf- und Einsichtsrechte von Aufsichtsbehörden und Prüfgesellschaften des Kunden, etwa der FINMA oder einer Finanzkontrolle, bleiben vorbehalten.

20.6 In *Triage* und *Extract* wird aufgezeichnet, welche Mitarbeiterin oder welcher Mitarbeiter der advact eine verdächtige E-Mail analysiert und bearbeitet hat. Im *Board* ist ersichtlich, wer eine E-Mail mit welchem Verdict abgeschlossen («resolved») hat; lesende Zugriffe von Analysten werden protokolliert.

20.7 Im advact Adminportal besteht ein unveränderbares Audit Log, das sämtliche Zugriffe von Mitarbeitenden der advact oder des Kunden auf E-Mail-Inhalte aufzeichnet. Wer auf den Inhalt einer E-Mail zugreifen will, muss eine Begründung angeben. Der Kunde hat vollen lesenden Zugriff auf das Audit Log. So ist jederzeit nachvollziehbar, wer zu welchem Zeitpunkt auf welche E-Mail-Inhalte zugegriffen hat.

21 Umgang mit rechtswidrigen Inhalten

21.1 Stellt advact bei der Analyse gemeldeter oder als verdächtig erkannter E-Mails Inhalte fest, die auf eine

Straftat hindeuten, informiert sie umgehend den vom Kunden bezeichneten SOC-Kontakt. Gemeint sind insbesondere Inhalte nach Art. 197 Abs. 4 und 5 StGB (verbotene Pornografie / CSAM) oder nach Art. 187 ff. StGB (sexuelle Handlungen mit Kindern). Eine Pflicht zur aktiven Suche nach solchen Inhalten besteht nicht.

21.2 advact ist berechtigt, den Fund zum eigenen Schutz über das Meldeformular des Bundesamts für Polizei (fedpol) zu melden. Die Vertraulichkeit gemäss Ziff. 11 steht dem nicht entgegen. Diese Meldung ersetzt keine Strafanzeige.

21.3 Kosten, die dem Kunden aus dem weiteren Umgang mit dem Fund entstehen, trägt der Kunde selbst, insbesondere Kosten einer Strafanzeige, eines Verfahrens oder einer Rechtsberatung.

22 Höhere Gewalt

22.1 Keine Partei haftet für die Nichterfüllung ihrer Pflichten, soweit diese auf Ereignisse zurückgeht, die sie trotz angemessener Vorkehrungen nicht verhindern konnte, etwa Naturereignisse, Pandemien, behördliche Anordnungen, Krieg, Terror, grossflächige Strom- oder Netzausfälle oder Cyberangriffe auf Dritte, die dem Stand der Technik entsprechende Massnahmen überwinden. Die betroffene Partei informiert die andere unverzüglich. Dauert das Ereignis länger als 30 Tage, kann jede Partei den Vertrag kündigen.

23 Sperrung aus Sicherheitsgründen

23.1 advact darf Zugänge oder einzelne Funktionen vorübergehend sperren, soweit dies zur Abwehr einer Gefahr für die Sicherheit der advact Services, des Kunden oder anderer Kunden, bei begründetem Verdacht auf Missbrauch oder aufgrund einer behördlichen Anordnung erforderlich ist. advact beschränkt die Sperrung auf das Nötige und informiert den Kunden unverzüglich.

24 Änderungen dieser AGB

24.1 advact kann diese AGB sowie die Leistungsbeschreibung mit Wirkung für die Zukunft ändern. Sie teilt Änderungen dem Kunden mindestens 30 Tage vor Inkrafttreten schriftlich mit.

24.2 Für laufende Verträge gelten Änderungen ab dem Beginn des nächsten Vertragsjahres. Änderungen, die aufgrund zwingender Rechtsänderungen oder zur Behebung von Sicherheitsrisiken nötig sind, oder Änderungen, die den Kunden nicht benachteiligen, können früher gelten, frühestens 30 Tage nach der Mitteilung.

24.3 Benachteiligt eine Änderung den Kunden, kann er den Vertrag auf das Inkrafttreten der Änderung kündigen. Kündigt er nicht, gilt die Änderung als genehmigt. advact weist in der Mitteilung auf diese Folge hin.

25 Schlussbestimmungen

- 25.1 Vereinbarungen zwischen den Parteien, etwa Angebote, Annahmen, Bestellungen und Einzelverträge sowie deren Änderungen und Ergänzungen, sind nur gültig, wenn sie schriftlich festgehalten werden. E-Mails sind der Schriftform gleichgestellt.
- 25.2 Mitteilungen an advact sind an info@advact.ch zu richten, Mitteilungen zu Datenschutz und Informationssicherheit an compliance@advact.ch. Mitteilungen an den Kunden gehen an die von ihm bezeichnete Ansprechperson.
- 25.3 Der Kunde darf Rechte und Pflichten aus dem Vertrag nur mit vorgängiger schriftlicher Zustimmung der advact übertragen. advact darf den Vertrag auf eine Rechtsnachfolgerin oder eine mit ihrer verbundenen Gesellschaft übertragen. Sie teilt dies dem Kunden vorgängig mit; der Kunde kann den Vertrag in diesem Fall auf den Zeitpunkt der Übertragung kündigen.
- 25.4 Sollte eine Bestimmung des Vertrags ganz oder teilweise unwirksam sein oder werden, bleibt die Gültigkeit der übrigen Bestimmungen unberührt. Die unwirksame Bestimmung wird durch eine wirksame ersetzt, die ihrem wirtschaftlichen Zweck möglichst nahekommt. Dasselbe gilt für allfällige Vertragslücken.
- 25.5 Bei Abweichungen zwischen der deutschen Fassung und Übersetzungen dieser AGB geht die deutsche Fassung vor.
- 25.6 Für Kunden mit einem bestehenden Lizenzvertrag und / oder laufenden Angebot über die advact Services gelten diese AGB ab der nächsten Verlängerung oder ab der Annahme eines neuen Angebots. Bis dahin gilt der bestehende Vertrag.
- 25.7 Der Vertrag untersteht schweizerischem materiellem Recht unter Ausschluss des Kollisionsrechts und des Übereinkommens der Vereinten Nationen über Verträge über den internationalen Warenkauf (CISG).
- 25.8 Ausschliesslicher Gerichtsstand ist Bern.

Bern, 01.11.2026 – advact AG