

Auftragsverarbeitungsvertrag

zwischen dem

Kunden der net.ter GmbH, nach Erhalt der Aktivierungsbestätigung

- nachstehend Auftraggeber genannt –

und dem / der

net.ter GmbH

Kaistr. 5

40221 Düsseldorf

- nachstehend Auftragnehmer genannt -

wird der folgende Vertrag zur Auftragsverarbeitung getroffen.

## Präambel

Sämtliche in diesem Vertrag beschriebenen Verpflichtungen finden Anwendung auf alle Tätigkeiten, die mit der Auftragserfüllung in Zusammenhang stehen und bei denen Mitarbeiterinnen und Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Auftragsverarbeiter mit personenbezogenen Daten des Auftraggebers in Berührung kommen bzw. kommen können.

Da hier eine gemeinsame Pflicht zur Regelung besteht, verpflichten sich Auftraggeber und Auftragnehmer diese Vereinbarung jeweils an das geltende o.g. Recht anzupassen.

## 1. Rechtsgrundlage, Begriffsbestimmungen

Für diesen Vertrag liegt die EU-DSGVO zu Grunde.

Sofern der Auftraggeber einem kirchlichen/ konfessionellen Datenschutzgesetz gem. Art. 91 EU-DSGVO unterliegt, erfolgt hierzu die folgende Erklärung der net.ter GmbH: Wir akzeptieren das für den Auftraggeber geltende Datenschutzgesetz. Wir werden mit der dortigen Aufsichtsbehörde zusammenarbeiten und unterwerfen uns dieser.

Es gelten die Begriffsbestimmungen entsprechend aus der oben genannten datenschutzrechtlichen Grundlage.

## 2. Gegenstand und Dauer des Auftrages

### Gegenstand

Gegenstand der Vereinbarung ist die Verarbeitung personenbezogener Daten (nachstehend „Daten“ genannt) durch den Auftragnehmer für den Auftraggeber in dessen Auftrag und nach dessen Weisung zur Durchführung des Awareness-Trainings für alle Mitarbeiter:innen. Dabei stellt der Auftraggeber dem Auftragnehmer die benötigten Daten zur Verfügung. Der Auftragnehmer führt seine Leistungen durch. Nach Ablauf der Nachweisfrist löscht der Auftragnehmer die Daten aus seinem System.

### Dauer

Die Dauer dieses Vertrags (Laufzeit) entspricht der Laufzeit des Dienstleistungsvertrages Datenschutz.

Der Vertrag gilt unbeschadet des vorstehenden Absatzes so lange, wie der Auftragnehmer personenbezogene Daten des Auftraggebers verarbeitet (einschließlich Backups).

Soweit sich aus anderen Vereinbarungen zwischen Auftraggeber und Auftragnehmer anderweitige Abreden zum Schutz personenbezogener Daten ergeben, soll dieser Vertrag zur Auftragsverarbeitung vorrangig gelten, es sei denn die Parteien vereinbaren ausdrücklich etwas anderes.

### 3. Datenverarbeitung im Auftrag

Die Art der Verarbeitung, der Zweck der Verarbeitung, die Art der Daten und die Kategorien der betroffenen Personen sind in Anlage 1 dieses Vertrages festgelegt.

### 4. Sicherheit der Verarbeitung

Der Auftragnehmer ergreift in seinem Verantwortungsbereich alle erforderlichen technisch-organisatorischen Maßnahmen zur Sicherstellung des Schutzes der personenbezogenen Daten und übergibt dem Auftraggeber die Dokumentation zur Prüfung (Anlage 2).

Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Vertrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

Die vereinbarten technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer zukünftig gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Über wesentliche Änderungen, die durch den Auftragnehmer zu dokumentieren sind, ist der Auftraggeber unverzüglich in Kenntnis zu setzen.

### 5. Rechte von betroffenen Personen

Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich mittels geeigneter technisch-organisatorischer Maßnahmen bei der Beantwortung und Umsetzung von Anträgen betroffener Personen hinsichtlich ihrer Datenschutzrechte. Er darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers beauskunften, portieren, berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten. Soweit vom Leistungsumfang umfasst, sind die Rechte auf Auskunft, Berichtigung, Einschränkung der Verarbeitung, Löschung sowie Datenportabilität nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

### 6. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Vertrags eigene gesetzliche Pflichten gemäß der DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

- a) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die berechtigterweise Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten, einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
- b) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- c) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Vertrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
- d) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten, einem anderen Anspruch

oder einem Informationsersuchen im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

- e) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.
- f) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse aufgrund dieses Vertrags.
- g) Der Auftragnehmer meldet Verletzungen des Schutzes personenbezogener Daten unverzüglich an den Auftraggeber in der Weise, dass der Auftraggeber seinen gesetzlichen Pflichten, insbesondere nach Art. 33, 34 DSGVO nachkommen kann. Er fertigt über den gesamten Vorgang eine Dokumentation an, die er dem Auftraggeber für weitere Maßnahmen zur Verfügung stellt.
- h) Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich im Rahmen bestehender Informationspflichten gegenüber Aufsichtsbehörden und Betroffenen und stellt ihm in diesem Zusammenhang sämtliche relevanten Informationen unverzüglich zur Verfügung.
- i) Soweit der Auftraggeber zur Durchführung einer Datenschutz-Folgenabschätzung verpflichtet ist, unterstützt ihn der Auftragnehmer unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen. Gleiches gilt für eine etwaig bestehende Pflicht zur Konsultation der zuständigen Datenschutz-Aufsichtsbehörde.

Dieser Vertrag entbindet den Auftragnehmer nicht von der Einhaltung anderer Vorgaben der DSGVO oder des hier zugrunde liegenden Gesetzes.

Datenschutzbeauftragte:r beim Auftragnehmer

Der Auftragnehmer hat einen Datenschutzbeauftragten benannt.

Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich schriftlich mitzuteilen. Der Auftragnehmer gewährleistet, dass die Anforderungen an den Datenschutzbeauftragten und seine Tätigkeit gemäß den rechtlichen Anforderungen erfüllt werden.

## 7. Unterauftragsverhältnisse

Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer in Anspruch nimmt, z.B. Telekommunikations-, Post-/Transport, Reinigungs- oder Bewachungsdienstleistungen. Wartungs- und Prüfleistungen stellen dann ein Unterauftragsverhältnis dar, wenn sie für IT-Systeme erbracht werden, die im Zusammenhang mit einer Leistung des Auftragnehmers nach diesem Vertrag stehen. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

Der Auftraggeber stimmt der Beauftragung der in Anlage 3 bezeichneten Unterauftragnehmer unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe der diesem Vertrag zugrunde liegenden rechtlichen Anforderungen mit dem Unterauftragnehmer zu. Die vertragliche Vereinbarung wird dem Auftraggeber auf dessen Verlangen vorgelegt, wobei geschäftliche Klauseln ohne datenschutzrechtlichen Bezug hiervon ausgenommen sind.

Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet. Die Einhaltung und Umsetzung der technisch-organisatorischen Maßnahmen beim Unterauftragnehmer wird unter Berücksichtigung des Risikos beim Unterauftragnehmer vorab der Verarbeitung personenbezogener Daten und

sodann regelmäßig durch den Auftragnehmer kontrolliert. Der Auftragnehmer stellt dem Auftraggeber die Kontrollergebnisse auf Anfrage zur Verfügung. Der Auftragnehmer stellt ferner sicher, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Kontrollrechte) auch direkt gegenüber den Unterauftragnehmern wahrnehmen kann.

Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher.

Eine weitere Auslagerung durch den Unterauftragnehmer ist nicht gestattet.

## 8. Internationale Datentransfers

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

## 9. Kontrollrechte des Auftraggebers

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

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

Der Nachweis der technisch-organisatorischen Maßnahmen zur Einhaltung der allgemeinen Anforderungen des Datenschutzes sowie der besonderen Anforderungen, die den Auftrag betreffen, kann erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln,
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren,
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzaudatoren, Qualitätsaudatoren) oder auch
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

## 10. Weisungsbefugnis des Auftraggebers

Der Auftragnehmer verarbeitet personenbezogene Daten nur auf Basis dokumentierter Weisungen des Auftraggebers, es sei denn er ist nach dem Recht des Mitgliedstaats oder nach Unionsrecht zu einer Verarbeitung verpflichtet. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform). Die anfänglichen Weisungen des Auftraggebers werden durch diesen Vertrag festgelegt. Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

## 11. Löschung und Rückgabe von personenbezogenen Daten

Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens aber mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

## 12. Zurückbehaltungsrecht

Die Einrede des Zurückbehaltungsrechts, gleich aus welchem Rechtsgrund, an den vertragsgegenständlichen Daten sowie an evtl. vorhandenen Datenträgern wird ausgeschlossen.

## 13. Rechtswahl, Gerichtsstand

Es gilt deutsches Recht. Gerichtsstand ist der Sitz des Auftraggebers.

Düsseldorf, 19.08.2024



Auftragnehmer

## Anlagen

Anlage 1: Art, Zweck, Art der Daten, Kategorien betroffener Personen

Anlage 2: Nachweis Sicherheit der Verarbeitung

Anlage 3: Unterauftragsverhältnisse beim Auftragnehmer zum Zeitpunkt der Auftragsvergabe

## Anlage 1

### Art und Zweck der vorgesehenen Verarbeitung von Daten

Der Auftragnehmer führt folgende Verarbeitungen im Auftrag des Auftraggebers durch:

- Erheben, Erfassen, Organisation, Ordnen,
- Speicherung, die Anpassung oder Veränderung,
- das Auslesen, das Abfragen, die Verwendung,
- den Abgleich oder die Verknüpfung,
- die Einschränkung, das Löschen oder die Vernichtung

Der Auftragnehmer erhält Zugriff auf die hier benannten personenbezogenen Daten (dadurch, dass der Auftraggeber ihm die Daten bereitstellt oder ihm einen Zugriff auf die Daten ermöglicht) bzw. der Auftraggeber erlaubt dem Auftragnehmer, die Daten zu verarbeiten.

### Art der Daten

- Name, Vorname der Teilnehmer:innen am Awareness-Training,
- E-Mail-Adresse der Teilnehmer:innen,
- Dokumentation der Teilnahme und des Erfolgs (Erkennen der Phishing-E-Mails).

### Besondere Kategorien von Daten

- keine besonderen Kategorien der Daten

### Kategorien betroffener Personen

Bei den Betroffenen der oben aufgelisteten Daten handelt es sich um:

- Beschäftigte, inkl. Auszubildende und ehrenamtlich Tätige

## Anlage 2: Sicherheit der Verarbeitung

Der Auftragnehmer stellt dem Auftraggeber die Anlage zur Sicherheit der Verarbeitung gerne auf Anfrage zur Verfügung. Anlage 3: Unterauftragsverhältnisse beim Auftragnehmer

Die folgenden Unterauftragsverhältnisse sind genehmigt:

| Firma /<br>Unterauftragnehmer | Anschrift<br>Land | Leistung im Rahmen<br>dieses Vertrages   | bei Drittland: geeignete<br>Garantien  |
|-------------------------------|-------------------|--|--|
| Hetzner GmbH                  | Deutschland       | Hosting des Servers für das<br>Awareness-Training                              | Keine Übermittlung in ein<br>Drittland |
| Sendinblue GmbH               | Deutschland       | Senden von E-Mails   | Keine Übermittlung in ein<br>Drittland |
| Microsoft GmbH                | Deutschland       | Speicherung der<br>Dokumentation nach<br>Abschluss des Awareness-<br>Trainings | Keine Übermittlung in ein<br>Drittland |