

Verpflichtungserklärung zur Vertraulichkeit und zum Datenschutz

VERPFLICHTENDE STELLE

Tobias Nase GmbH, Kronstädter Str. 20, 50858 Köln, eingetragen beim Amtsgericht Köln unter HRB 123307, vertreten durch den Geschäftsführer Tobias Nase (nachfolgend „Gesellschaft“)

VERPFLICHTETE PERSON

Name, Vorname

Beginn der Tätigkeit

Anschrift (Straße, Hausnummer, PLZ, Ort)

Rolle

☐

Mitarbeiter

☐

Freelancer

☐

Sonstige: _____

Die Gesellschaft entwickelt und betreibt die Vertriebssoftware ClosingHub und verarbeitet dabei personenbezogene Daten im Auftrag ihrer Kunden. Im Vertrag zur Auftragsverarbeitung hat sie zugesagt, nur Personen einzusetzen, die vor Beginn ihrer Tätigkeit zur Vertraulichkeit verpflichtet und mit den einschlägigen Vorschriften vertraut sind. Mit dieser Erklärung verpflichtet sich die oben genannte Person (nachfolgend „verpflichtete Person“) dazu.

1. Geltungsbereich

- 1.1** Die Erklärung gilt für jede Tätigkeit für die Gesellschaft, im Arbeitsverhältnis ebenso wie in freier Mitarbeit, und unabhängig davon, ob die verpflichtete Person im Einzelfall Zugang zu personenbezogenen Daten hat.
- 1.2** Sie erfasst alle Informationen, die der verpflichteten Person durch ihre Tätigkeit bekannt werden, gleich in welcher Form: im Quellcode, in der Datenbank, in Protokollen, in Dokumenten, in Gesprächen oder auf Bildschirmen.
- 1.3** Weitergehende Pflichten aus dem Arbeitsvertrag oder dem Dienstvertrag bleiben unberührt.

2. Vertraulichkeit personenbezogener Daten

- 2.1** Die verpflichtete Person wahrt die Vertraulichkeit personenbezogener Daten. Sie verarbeitet sie nur, soweit es für die ihr übertragene Aufgabe erforderlich ist, und schützt sie vor unbefugtem Zugriff, Verlust und Veränderung (Art. 5 Abs. 1 lit. f und Art. 32 Abs. 4 DSGVO).
- 2.2** Daten der Kunden verarbeitet sie ausschließlich auf Weisung der Gesellschaft, die ihrerseits nur auf dokumentierte Weisung des jeweiligen Kunden handelt (Art. 28 Abs. 3 lit. b und Art. 29 DSGVO). Eine Nutzung für eigene Zwecke oder für Zwecke Dritter ist ausgeschlossen.
- 2.3** Zugriffe auf Arbeitsbereiche von Kunden erfolgen nur über die dafür vorgesehenen Funktionen mit Zweckangabe. Ein allgemeiner Lesezugriff auf Kundendaten wird nicht hergestellt. Tests laufen auf Testdaten, nie auf Kopien von Betriebsdaten.
- 2.4** Hält die verpflichtete Person eine Weisung für rechtswidrig, teilt sie dies dem Geschäftsführer unverzüglich mit.

3. Geschäfts- und Betriebsgeheimnisse

3.1 Vertraulich sind alle nicht öffentlichen Informationen über die Gesellschaft, ihre Produkte und ihre Kunden, insbesondere Quellcode, Aufbau und Abläufe der Software, Zugangsdaten und Schlüssel, Kunden- und Preisdaten, Geschäftszahlen, Pläne und unveröffentlichte Funktionen. Sie sind Geschäftsgeheimnisse im Sinne des Gesetzes zum Schutz von Geschäftsgeheimnissen (GeschGehG).

3.2 Die verpflichtete Person nutzt sie ausschließlich für ihre Aufgabe und gibt sie nicht an Dritte weiter. Bildschirmfotos, Code-Ausschnitte oder Beschreibungen der Software veröffentlicht sie nur mit vorheriger Zustimmung der Gesellschaft.

3.3 Ausgenommen sind Informationen, die ohne ihr Zutun öffentlich bekannt sind oder die sie nachweislich unabhängig und rechtmäßig erhalten hat. Gesetzlich erlaubte Offenlegungen, etwa nach § 5 GeschGehG oder dem Hinweisgeberschutzgesetz, bleiben unberührt.

4. Fernmeldegeheimnis

4.1 ClosingHub baut für Kunden Telefongespräche auf, führt sie durch und rechnet sie ab. Soweit die verpflichtete Person daran mitwirkt, wahrt sie das Fernmeldegeheimnis nach § 3 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes (TDDDG, bis Mai 2024 TTDG). Es umfasst den Inhalt der Gespräche und ihre näheren Umstände, insbesondere ob jemand an einem Gespräch beteiligt ist oder war.

4.2 Sie verschafft sich und anderen keine Kenntnis vom Inhalt oder von den näheren Umständen der Gespräche über das hinaus, was für den Betrieb der Telefonie einschließlich des Schutzes der technischen Systeme erforderlich ist. Sie hört keine Gespräche mit und zeichnet keine auf.

5. Keine Weitergabe an KI-Werkzeuge und Dritte

5.1 Personenbezogene Daten aus Arbeitsbereichen von Kunden gibt die verpflichtete Person in kein KI-Werkzeug ein, weder in Chat-Assistenten noch in Programmierhilfen, Übersetzungs- oder Transkriptionsdienste. Dazu zählen Leads, Kontakte, Notizen, Gespräche, Unterlagen sowie Namen und Adressen von Nutzern der Kunden. Erlaubt sind Angaben ohne Personenbezug, etwa Datenbankschema, Zählungen und technische Kennungen.

5.2 Andere vertrauliche Informationen, etwa Quellcode, gibt sie nur in Werkzeuge ein, die die Gesellschaft freigegeben hat, und nur nach deren Regeln.

5.3 An sonstige Dritte gelangen Daten nur über die Dienstleister und Wege, die im Vertrag zur Auftragsverarbeitung genannt sind. Private Konten, Messenger, Cloud-Speicher und E-Mail-Postfächer sind dafür ausgeschlossen.

5.4 Bildschirmfotos für Fehlerbeschreibungen stammen aus Test- oder Demo-Arbeitsbereichen, nicht aus Arbeitsbereichen von Kunden.

6. Zugänge, Geräte und Kopien

6.1 Die verpflichtete Person erhält eigene, persönliche Zugänge. Sie gibt Zugangsdaten nicht weiter, nutzt keine fremden Zugänge und bewahrt Passwörter und Schlüssel nur in einem Passwortmanager oder einem vergleichbar geschützten Speicher auf.

6.2 Auf allen Konten mit Zugang zu Systemen der Gesellschaft ist die Anmeldung mit zweitem Faktor eingeschaltet.

6.3 Sie arbeitet ausschließlich in den Repositories, Konten und Werkzeugen, die die Gesellschaft bereitstellt. Kopien von Quellcode oder Daten auf privaten Konten, privaten Repositories, privaten Datenträgern oder fremden Diensten legt sie nicht an.

6.4 Geräte, mit denen sie arbeitet, sind mit Kennwort und Bildschirmsperre geschützt und werden beim Verlassen gesperrt.

7. Meldung von Datenpannen

7.1 Bemerkt die verpflichtete Person eine Verletzung des Schutzes personenbezogener Daten oder hat sie den Verdacht darauf, meldet sie dies unverzüglich dem Geschäftsführer Tobias Nase, telefonisch und zusätzlich in Textform, ohne eine eigene Nachprüfung abzuwarten. Beispiele sind ein Fehlversand, ein verlorenes Gerät, offengelegte Zugangsdaten, ein unberechtigter Zugriff oder versehentlich gelöschte Daten.

7.2 Die Gesellschaft muss betroffene Kunden spätestens 24 Stunden nach Kenntnis informieren (Ziffer 14 des Vertrags zur Auftragsverarbeitung), die Kunden ihrerseits die Aufsichtsbehörde möglichst binnen 72 Stunden (Art. 33 DSGVO). Jede Verzögerung bei der ersten Meldung verkürzt diese Fristen.

7.3 Die Meldung enthält, soweit bekannt, was wann geschehen ist, welche Daten und ungefähr wie viele Personen betroffen sind und was bereits unternommen wurde. Spuren werden nicht beseitigt. Kunden oder Dritte informiert die verpflichtete Person nicht eigenmächtig.

8. Ende der Tätigkeit

8.1 Endet die Tätigkeit, gibt die verpflichtete Person alle Unterlagen, Datenträger, Zugänge und Arbeitsergebnisse unverzüglich zurück, löscht verbliebene Kopien und bestätigt die Löschung in Textform.

8.2 Zugänge werden spätestens am letzten Tag der Tätigkeit gesperrt.

9. Fortgeltung

Die Pflichten aus dieser Erklärung gelten nach dem Ende der Tätigkeit unbefristet fort.

10. Folgen von Verstößen

10.1 Verstöße gegen den Datenschutz können gegen die Gesellschaft Geldbußen nach Art. 83 DSGVO auslösen. Für die handelnde Person kommen nach Art. 84 DSGVO in Verbindung mit § 42 BDSG Freiheits- oder Geldstrafen in Betracht.

10.2 Die Verletzung von Geschäftsgeheimnissen kann nach § 23 GeschGehG strafbar sein, die Verletzung des Fernmeldegeheimnisses nach § 206 StGB.

10.3 Im Arbeitsverhältnis kann ein Verstoß arbeitsrechtliche Folgen bis zur Kündigung haben, in freier Mitarbeit die Kündigung des Vertrags. Ansprüche auf Unterlassung und Schadensersatz bleiben unberührt, ebenso eine vertraglich vereinbarte Vertragsstrafe.

11. Bestätigung

Die verpflichtete Person bestätigt, diese Erklärung und das Merkblatt in der Anlage erhalten und gelesen zu haben. Sie hatte Gelegenheit, Fragen zu stellen. Je eine unterschriebene Ausfertigung erhalten die verpflichtete Person und die Gesellschaft.

VERPFLICHTETE PERSON

Ort, Datum

Unterschrift

Name in Druckschrift: _____

FÜR DIE TOBIAS NASE GMBH

Ort, Datum

Unterschrift

Tobias Nase, Geschäftsführer

Anlage: Merkblatt mit den wichtigsten Vorschriften

Zusammenfassungen in eigenen Worten. Maßgeblich ist allein der jeweils gültige Gesetzestext, abrufbar unter gesetze-im-internet.de und eur-lex.europa.eu.

Datenschutz-Grundverordnung (DSGVO)

- Art. 5 Abs. 1 lit. f** Personenbezogene Daten sind so zu verarbeiten, dass ihre Sicherheit angemessen gewährleistet ist, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung, Verlust, Zerstörung oder Schädigung (Integrität und Vertraulichkeit).
- Art. 28 Abs. 3 lit. b** Ein Auftragsverarbeiter muss gewährleisten, dass die zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet sind oder einer gesetzlichen Verschwiegenheitspflicht unterliegen.
- Art. 29** Wer einem Verantwortlichen oder Auftragsverarbeiter unterstellt ist und Zugang zu personenbezogenen Daten hat, verarbeitet sie ausschließlich auf dessen Weisung, es sei denn, das Recht der Union oder eines Mitgliedstaats verpflichtet dazu.
- Art. 32 Abs. 4** Verantwortliche und Auftragsverarbeiter stellen sicher, dass ihnen unterstellte Personen mit Zugang zu Daten diese nur auf Anweisung verarbeiten.
- Art. 33** Eine Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche möglichst binnen 72 Stunden der Aufsichtsbehörde. Der Auftragsverarbeiter meldet sie dem Verantwortlichen unverzüglich.
- Art. 83** Geldbußen bis 10 Mio. Euro oder 2 % des weltweiten Jahresumsatzes, bei bestimmten Verstößen bis 20 Mio. Euro oder 4 %, jeweils der höhere Betrag.
- Art. 84** Die Mitgliedstaaten legen weitere Sanktionen fest, in Deutschland unter anderem in §§ 42 und 43 BDSG.

Bundesdatenschutzgesetz (BDSG)

- § 42 Abs. 1** Freiheitsstrafe bis zu drei Jahren oder Geldstrafe für den, der wissentlich nicht allgemein zugängliche personenbezogene Daten einer großen Zahl von Personen ohne Berechtigung einem Dritten übermittelt oder zugänglich macht und dabei gewerbsmäßig handelt.
- § 42 Abs. 2, 3** Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe für den, der solche Daten ohne Berechtigung verarbeitet oder durch unrichtige Angaben erschleicht und dabei gegen Entgelt oder mit Bereicherungs- oder Schädigungsabsicht handelt. Verfolgt wird auf Antrag, unter anderem der betroffenen Person, des Verantwortlichen oder der Aufsichtsbehörde.

Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG)

- § 3** Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Verpflichtet sind die Anbieter und alle, die bei der Erbringung der Dienste mitwirken, auch nach dem Ende ihrer Tätigkeit. Kenntnis über das Erforderliche hinaus darf sich niemand verschaffen.

Strafgesetzbuch (StGB)

- § 206 Abs. 1** Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe für Inhaber oder Beschäftigte eines Unternehmens, das geschäftsmäßig Post- oder Telekommunikationsdienste erbringt, wenn sie unbefugt Tatsachen mitteilen, die dem Fernmeldegeheimnis unterliegen.

Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG)

- § 2 Nr. 1** Geschäftsgeheimnis ist eine Information, die nicht allgemein bekannt oder ohne Weiteres zugänglich ist, daher wirtschaftlichen Wert hat, durch angemessene Maßnahmen geschützt wird und an deren Geheimhaltung ein berechtigtes Interesse besteht.
- §§ 4, 5** Geschäftsgeheimnisse dürfen nicht unbefugt erlangt, genutzt oder offengelegt werden, insbesondere nicht entgegen einer Pflicht zur Geheimhaltung. Ausnahmen gelten etwa zur Aufdeckung rechtswidriger Handlungen, wenn dies dem öffentlichen Interesse dient.
- § 23** Freiheitsstrafe bis zu drei Jahren oder Geldstrafe, wenn ein Geschäftsgeheimnis aus Eigennutz, zugunsten Dritter, zur Förderung des Wettbewerbs oder in Schädigungsabsicht unbefugt erlangt, genutzt oder offengelegt wird. Verfolgt wird in der Regel auf Antrag.