TRASER Software GmbH | Christianspries 4 | 24159 Kiel

Auftragsverarbeitungsvertrag

1. Anwendungsbereich

Diese Anlage zur Auftragsverarbeitung gilt für alle aktuellen und zukünftigen Produkte & Leistungen der TRASER Software GmbH, Christianspries 4, 24159 Kiel (nachfolgend Auftragnehmer). Bei der Erbringung der Leistungen gemäß dem Hauptvertrag verarbeitet der Auftragnehmer personenbezogene Daten, die der Auftraggeber zur Erbringung der Leistungen zur Verfügung gestellt hat und bezüglich derer der Auftraggeber als Verantwortlicher im datenschutzrechtlichen Sinn fungiert („Auftraggeber-Daten"). Diese Anlage spezifiziert die Datenschutzpflichten und -rechte der Parteien im Zusammenhang mit der Verarbeitung der Auftraggeber-Daten zur Erbringung der Leistungen nach dem Hauptvertrag.

2. Umfang der Beauftragung/Weisungsbefugnisse des Auftraggebers

2.1 Der Auftragnehmer wird die Auftraggeber-Daten ausschließlich im Auftrag und gemäß den Weisungen des Auftraggebers verarbeiten, sofern der Auftragnehmer nicht gesetzlich dazu verpflichtet ist. In letzterem Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Gesetz eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

2.2 Die Verarbeitung von Auftraggeber-Daten durch den Auftragnehmer erfolgt ausschließlich in der Art, dem Umfang und zu dem Zweck wie im Anhang zu dieser Anlage spezifiziert; die Verarbeitung betrifft ausschließlich die darin bezeichneten Arten personenbezogener Daten und Kategorien betroffener Personen.

2.3 Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrages.

2.4 Der Auftraggeber behält sich das Recht zur Erteilung von Weisungen über Art, Umfang, Zwecke und Mittel der Verarbeitung von Auftraggeber-Daten vor.

Geschäftsführung
Hauke Lamb & Torben Weber
Amtsgericht Kiel
HRB 16053 KI

www.traser-software.de
info@traser-software.de
Tel.: +49 431 22 13 99 10
Fax: +49 431 22 13 99 30

Kieler Volksbank
IBAN: DE52 2109 0007 0056 0953 09
BIC: GENODEF1KIL
USt-ID: DE296134491

3. Anforderungen an Personal

3.1 Der Auftragnehmer hat alle Personen, die Auftraggeber-Daten verarbeiten, bezüglich der Verarbeitung von Auftraggeber-Daten zur Vertraulichkeit zu verpflichten.

3.2 Der Auftragnehmer stellt sicher, dass ihm unterstellte natürliche Personen, die Zugang zu Auftraggeber-Daten haben, diese nur auf seine Anweisung verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

4. Sicherheit der Verarbeitung

4.1 Der Auftragnehmer ergreift alle geeigneten technischen und organisatorischen Maßnahmen, die unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung der Auftraggeber-Daten sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen erforderlich sind, um ein dem Risiko angemessenes Schutzniveau für die Auftraggeber-Daten zu gewährleisten.

4.2 Dem Auftragnehmer ist es gestattet, technische und organisatorische Maßnahmen während der Laufzeit des Vertrages zu ändern oder anzupassen, solange sie weiterhin den gesetzlichen Anforderungen genügen.

5. Inanspruchnahme weiterer Auftragsverarbeiter

5.1 Der Auftraggeber genehmigt hiermit in allgemeiner Weise die Inanspruchnahme weiterer Auftragsverarbeiter durch den Auftragnehmer. Die gegenwärtig vom Auftragnehmer eingesetzten weiteren Auftragsverarbeiter sind im Anhang genannt.

5.2 Der Auftragnehmer wird den Auftraggeber über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder Ersetzung weiterer Auftragsverarbeiter informieren. Dem Auftraggeber steht im Einzelfall ein Recht zu, Einspruch gegen die Beauftragung eines potentiellen weiteren Auftragsverarbeiters zu erheben. Ein Einspruch darf vom Auftraggeber nur aus wichtigem, dem Auftragnehmer nachzuweisenden Grund erhoben werden. Soweit der Auftraggeber nicht innerhalb von 28 Tagen nach Zugang der Benachrichtigung Einspruch erhebt, erlischt sein Einspruchsrecht bezüglich der entsprechenden Beauftragung. Erhebt der Auftraggeber Einspruch, ist der

Auftragnehmer berechtigt, den Hauptvertrag und diesen Vertrag mit einer Frist von 3 Monaten zu kündigen.

5.3 Der Auftragnehmer wird jedem weiteren Auftragsverarbeiter vertraglich dieselben Datenschutzpflichten auferlegen, die in dieser Anlage in Bezug auf den Auftragnehmer festgelegt sind.

5.4 Der Auftragnehmer wird vor jeder Beauftragung sowie regelmäßig während der Beauftragung überprüfen, dass die weiteren Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen ergriffen haben und diese so durchgeführt werden, dass die Verarbeitung der Auftraggeber-Daten gemäß dieser Anlage erfolgt.

6. Rechte der betroffenen Personen

6.1 Der Auftragnehmer wird den Auftraggeber im Rahmen des Zumutbaren mit technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der ihnen zustehenden Rechte betroffener Personen nachzukommen.

6.2 Der Auftragnehmer wird insbesondere:

- den Auftraggeber unverzüglich informieren, falls sich eine betroffene Person mit einem Antrag auf Wahrnehmung ihrer Rechte in Bezug auf Auftraggeber-Daten unmittelbar an den Auftragnehmer wenden sollte;
- dem Auftraggeber auf Anfrage alle bei ihm vorhandenen Informationen über die Verarbeitung von Auftraggeber-Daten geben, die der Auftraggeber zur Beantwortung des Antrags einer betroffenen Person benötigt und über die der Auftraggeber nicht selbst verfügt.

7. Sonstige Unterstützungspflichten des Auftragnehmers

7.1 Der Auftragnehmer meldet dem Auftraggeber, unverzüglich nachdem ihm eine solche bekannt geworden ist, jede Verletzung des Schutzes von Auftraggeber-Daten, insbesondere Vorkommnisse, die zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu Auftraggeber-Daten führen. Die Meldung enthält nach Möglichkeit eine Beschreibung:

- der Art der Verletzung des Schutzes der Auftraggeber-Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
- der wahrscheinlichen Folgen der Verletzung des Schutzes der Auftraggeber-Daten;

– der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes der Auftraggeber-Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

7.2 Für den Fall, dass der Auftraggeber verpflichtet ist, die Aufsichtsbehörden und/oder Betroffenen nach Art. 33, 34 DSGVO zu informieren, wird der Auftragnehmer den Auftraggeber auf dessen Anfrage unterstützen, diese Pflichten einzuhalten.

7.3 Der Auftragnehmer wird den Auftraggeber im Rahmen des Zumutbaren bei etwa von ihm durchzuführenden Datenschutz-Folgenabschätzungen und sich gegebenenfalls anschließenden Konsultationen der Aufsichtsbehörden nach Art. 35, 36 DSGVO unterstützen.

8. Datenlöschung und -zurückgabe

Der Auftragnehmer wird auf die Weisung des Auftraggebers hin mit Beendigung des Hauptvertrages alle Auftraggeber-Daten entweder vollständig und unwiderruflich löschen oder an den Auftraggeber zurückgeben, sofern nicht gesetzlich eine Verpflichtung des Auftragnehmers zur weiteren Speicherung der Auftraggeber-Daten besteht.

9. Nachweise und Überprüfungen

9.1 Der Auftragnehmer wird dem Auftraggeber auf dessen Anforderung alle erforderlichen und beim Auftragnehmer vorhandenen Informationen zum Nachweis der Einhaltung seiner Pflichten nach diesem Vertrag zur Verfügung stellen.

9.2 Der Auftraggeber ist berechtigt, den Auftragnehmer bezüglich der Einhaltung der Regelungen dieses Vertrages, insbesondere der Umsetzung der technischen und organisatorischen Maßnahmen, zu überprüfen; einschließlich durch Inspektionen.

9.3 Nach Wahl des Auftragnehmers kann der Nachweis der Einhaltung der Pflichten nach diesem Vertrage anstatt durch eine Inspektion auch durch die Vorlage eines geeigneten, aktuellen Testats oder Berichts einer unabhängigen Instanz (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren oder Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit - z.B. nach BSI-Grundschutz - („Prüfungsbericht“) erbracht werden, wenn der Prüfungsbericht es dem Auftraggeber in angemessener Weise ermöglicht, sich von der Einhaltung der Vertragspflichten zu überzeugen.

Anhang

1. Art, Umfang und Zweck der Datenverarbeitung

Art und Zweck der Verarbeitung ergeben sich aus der gewählten Leistung, insbesondere:

— Zurverfügungstellung und Hosting von IT-Systemen (insbesondere Branchenlösungen und Microsoft-Produkte)

  Art der Daten:

  — Personenstammdaten
  — Kommunikationsdaten (z.B. Telefon, E-Mail)
  — Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
  — Kundenhistorie
  — Vertragsabrechnungs- und Zahlungsdaten

— Wartung/Support der IT-Systeme (insbesondere Branchenlösungen und Microsoft-Produkte) mit theoretischer Zugriffsmöglichkeit, die allerdings explizit untersagt und nicht gewünscht ist; Daten werden allenfalls im Rahmen der Wartung der IT-Systeme beiläufig ohne gewollte Verarbeitung seitens des Auftragnehmers zur Kenntnis genommen

  Art der Daten:

  — theoretischer/beiläufiger, nicht aber gewollter/zweckgerichteter Zugriff auf Daten aus:
    — IT-System (insbesondere Branchenlösungen und Microsoft-Produkte)
      - Personenstammdaten
      - Kommunikationsdaten (z.B. Telefon, E-Mail)
      - Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
      - Kundenhistorie
      - Vertragsabrechnungs- und Zahlungsdaten

Kategorien betroffener Personen:

— Kunden
— Interessenten
— Beschäftigte
— Dienstleister
— Lieferanten
— Handelsvertreter
— Ansprechpartner

2. Unterauftragsnehmer

— Leistung: Microsoft Azure Cloud Computing-Plattform und -Dienste
Firma Unterauftragnehmer: Microsoft Ireland Operations Ltd, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland

— Leistung: Hosting-Leistungen
Firma Unterauftragnehmer: Quattro Business Solutions DACH GmbH, Schellerdamm 4, 21079 Hamburg

— Leistung: Support Tool
Firma Unterauftragnehmer: Zendesk Inc., 989 Market St., CA 94103 San Francisco USA

— Leistung: Fernwartungs-Tool, Planio
Firma Unterauftragnehmer: Planio GmbH, Rudolfstr. 14, 10245 Berlin

— Leistung: Fernwartungs-Tool, Microsoft Teams
Firma Unterauftragnehmer: Microsoft Ireland Operations Ltd, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland

— Leistung: Fernwartungs-Tool, TeamViewer
Firma Unterauftragnehmer: TeamViewer Germany GmbH, Bahnhofsplatz 2, 73033 Göppingen

— Leistung: Entwicklungstool JIRA und Confluence
Firma Unterauftragnehmer: Atassian, Singel 236, 1016 AB Amsterdam Netherlands

— Leistung: 2nd Level Support Modul: akquinet- Zahlungsverkehr
Firma Unterauftragnehmer: Akquinet Dynamics Solution GmbH, Bollhörnkai 1, 24103 Kiel

— Leistung: 2nd Level Support Modul: Armada EQM Rental- Mietmodul
Firma Unterauftragnehmer: Armada Dynamics AS, Sandakerveien 52, 0477 Oslo

— Leistung: 2nd Level Support Modul: Anveo Elektronischer- Datenaustausch
Firma Unterauftragnehmer: Conion media GmbH, Fruchtallee 23a, 202059 Hamburg

— Leistung: 2nd Level Support Modul: document capture- Continia Software Firma Unterauftragnehmer: Continia Software GmbH, Mittelweg 144, DE 20148 Hamburg

— Leistung: 2nd Level Support Modul: crefodynamics- Wirtschaftsauskünfte
Firma Unterauftragnehmer: COSMO CONSULT AG, Schönberger Straße 15, 10963 Berlin

— Leistung: 2nd Level Support Modul: dime.Sheduler- Werkstattplanung
Firma Unterauftragnehmer: Dime CVBA, Katwilgweg 2, 2050 Antwerpen

— Leistung: 2nd Level Support Modul: Spindle- Dokumentenversand
Firma Unterauftragnehmer: Draycir Ltd, 1-3 De Montfort, Mews Leicester LE1 7FW

— Leistung: 2nd Level Support Modul: OPplus- Zahlungsverkehr
Firma Unterauftragnehmer: gbedv GmbH & Co. KG, Am Kiel- Kanal 1, 24106 Kiel

— Leistung: 2nd Level Support Modul: JetReports- BI-Lösung
Firma Unterauftragnehmer: JetReports Deutschland GmbH, Hutfilterstr. 16-18, 28195 Bremen

— Leistung: 2nd Level Support NAV

Firma Unterauftragnehmer: Kepler Management Systems SRL, Strada Gheorghe Matac 33-35 sector 2, Bucaresti CP 020341

— Leistung: 2nd Level Support Modul: Lessor- Lohn /Gehalt
Firma Unterauftragnehmer: Lessor GmbH, Kokkolastraße 2, 40882 Ratingen

— Leistung: 2nd Level Support Modul: NAVconnect- Basis / Shopware
Firma Unterauftragnehmer: m+p business, Gablonzstr. 2, 38114 Braunschweig

— Leistung: 2nd Level Support Modul: Easy Security- Sicherheitssoftware
Firma Unterauftragnehmer: Mergetool.com, 3577 Chamblee Tucker Rd., Suite A- Box 279

— Leistung: 2nd Level Support TRASER Cloud Bereitstellungen
Firma Unterauftragnehmer: Microsoft Ireland Operations Ltd., Sandyford Industrial Estat, 5678 Dublin

— Leistung: 2nd Level Support Modul: DATEV-Finanzsoftware
Firma Unterauftragnehmer: Sievers-SNC, Hans-Wunderlich-Str. 8, 49078 Osnabrück

— Leistung: 2nd Level Support Modul: TempVision- Zeitwirtschaft
Firma Unterauftragnehmer: Tempras GmbH & Co.KG, Dierdorfer Landstraße 10, 56242 Selters

— Leistung: 2nd Level Support Modul: DSGVO Toolbox
Firma Unterauftragnehmer: TSO Data GmbH, Business-Systemhaus, Preußenweg 10, 49076 Osnabrück

3. Technische und organisatorische Maßnahmen

Nr.	Gebiet	Beschreibung
1.	**Allgemeine organisatorische Maßnahmen zum Datenschutz**	
	Wie ist die Umsetzung des Datenschutzes organisiert?	Ein externer Datenschutzbeauftragter wird zur Wahrnehmung der Beratungs- und Kontrollfunktionen aus dem DSGVO eingesetzt.
	Nennen Sie uns bitte den Namen und die Kontaktdaten Ihres Datenschutzbeauftragten.	IT-Kanzlei Kiel Inhaber Rechtsanwalt Niels Köhrer Schauenburgerstraße 36 24105 Kiel T: 0431 647368-20 F: 0431 2596621 Mail: kontakt@it-kanzlei-kiel.de

	In welcher Form werden die Mitarbeiter auf die Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen geschult, die für diese Verarbeitung in Anwendung kommen?	-Regelmäßige Datenschutzschulungen aller Mitarbeiter -Verpflichtung aller Mitarbeiter auf die Datenschutzerklärung
	Sind die Verarbeitungen hinsichtlich datenschutzrechtlicher Zulässigkeit dokumentiert?	Ja, im Rahmen des internen Verfahrens-verzeichnisses sind die Datenströme dokumentiert und die Zulässigkeit der Verarbeitung und Nutzung nach DSGVO nachgewiesen.
1.1	**Zutrittskontrolle**	
	Wie werden die Gebäude, in denen die Verarbeitung stattfindet, vor unbefugtem Zutritt gesichert?	Alarmanlage in Gebäudeanteil der Firma. Das Gelände ist videoüberwacht.
	Wie werden die Räume / Büros, in denen die Verarbeitung stattfindet, vor unbefugtem Zutritt gesichert?	Sicherungskreise der Alarmanlage. Zutritt nur für Mitarbeiter per dediziertem RFID-Chip. Der Zutritt und Aufenthalt von Besuchern erfolgt nur in Begleitung des verantwortlichen Firmenpersonals.
1.2	**Zugangskontrolle**	
	Wie wird die Gültigkeit von Benutzerzugängen überprüft?	Die Abteilungsleiter bzw. Geschäftsführer sind verpflichtet, relevante Änderungen in Beschäftigungsverhältnissen rechtzeitig der Administration anzuzeigen. Nicht mehr benötigte Benutzerkonten und Zugriffsrechte werden umgehend entzogen.
	Wie sind die mobilen IT- Geräte gesichert?	Die Geräte sind so eingestellt, dass eine Eingabe eines Passwortes erforderlich ist.
	Wie wird sichergestellt, dass die Anzahl von Administrationszugängen ausschließlich auf die notwendige Anzahl reduziert ist und nur fachlich und persönlich geeignetes Personal hierfür eingesetzt wird?	Administrationszugänge erhalten nur dedizierte Systemadministratoren und deren Vertretungen aufgrund einer Genehmigung durch die Geschäftsführung.
1.3	**Zugriffskontrolle**	

	Wie wird erreicht, dass Passwörter nur dem jeweiligen Benutzer bekannt sind?	Es existieren keine gemeinsam genutzten Benutzerzugänge. Die Benutzer erhalten ein individuelles Initial-Passwort. Eine Änderung des Passwortes wird bei der Anmeldung technisch erzwungen. Die Mitarbeiter werden bei der Einstellung unterwiesen, sorgsam mit Passwörtern umzugehen und diese nicht anderen Personen zugänglich zu machen.
	Welche Anforderungen werden an die Komplexität von Passwörtern gestellt?	Das Kennwort besteht aus mindestens 8 Zeichen. Ebenso sind Sonderzeichen und Ziffern zwingend erforderlich.
	Welche zusätzlichen Authentifizierungsmechanismen werden neben dem Passwort verwendet?	Durch Gruppenrichtlinien wird die Verwendung eines mobilen Endgeräts für eine Multi-Faktor-Authentifizierung per SMS oder Authenticator-App zusätzlich zum Passwort erzwungen.
	Welche organisatorischen Vorkehrungen werden zur Verhinderung von unberechtigten Zugriffen auf personenbezogene Daten am Arbeitsplatz getroffen?	Zugriffsfreigaben erfolgen User- und Gruppen-basiert für die mit der Verarbeitung betrauten Personen. Die Systeme sind passwortgeschützt. Arbeitsplätze werden automatisch bei Inaktivität gesperrt. Die Mitarbeiter sind unterwiesen, bei Verlassen des Arbeitsplatzes ihre Arbeitsplätze zu sperren und keine sichtbaren bzw. frei zugängliche personenbezogene Daten zu hinterlassen.
1.4	**Weitergabekontrolle**	
	Wie gewährleisten Sie die Integrität und Vertraulichkeit bei der Weitergabe von personenbezogenen Daten?	Die Weitergabe erfolgt über verschlüsselte Kanäle und/oder die Verschlüsselung der Daten selbst.
	Wie wird der unberechtigte Abfluss von personenbezogenen Daten durch technische Maßnahmen beschränkt?	Eine strikte Rechtevergabe sichert die Daten vor unberechtigtem Zugriff.
1.5	**Eingabekontrolle**	

	Welche Maßnahmen werden ergriffen, um nachvollziehen zu können, wer wann und wie lange auf Applikationen zugegriffen hat?	Zugriffs-Logs der Server und Systeme.
	Wie ist nachvollziehbar, welche Aktivitäten auf den entsprechenden Applikationen durchgeführt wurden?	Ereignislogs der Server und Anwendungen.
	Welche Maßnahmen werden ergriffen, damit die Verarbeitung durch die Mitarbeiter nur gemäß der Weisungen des Auftraggebers erfolgen kann?	Schulung bzw. Sensibilisierung der Mitarbeiter durch regelmäßige Veranstaltungen bzw. Personalgespräche.
	Welche Maßnahmen werden getroffen, damit auch Unterauftragnehmer ausschließlich im vereinbarten Umfang personenbezogene Daten des Auftraggebers durchführt?	Die Datenverarbeitung von Unterauftragnehmern erfolgt mit eindeutigen Auftragsdefinitionen und einer formalisierten Auftragserteilung. Unterauftragnehmer halten in der Regel ein Testat für die Einhaltung über den rechtskonformen Umgang mit personenbezogenen Daten vor.
1.6	**Verfügbarkeitskontrolle**	
	Wie wird gewährleistet, dass die Datenträger vor elementaren Einflüssen (Feuer, Wasser, elektromagnetische Abstrahlung etc.) geschützt sind?	Tägliche Backups auf einen räumlich getrennten Server schützen vor Datenverlust.
	Welche Schutzmaßnahmen werden zur Bekämpfung von Schadprogrammen eingesetzt und wie wird deren Aktualität gewährleistet?	Betriebssystem-Sicherheitsupdates und Antiviren-Software und –Definitionen werden zentral automatisiert ausgerollt und aktualisiert. Antiviren- und Firewall-Lösungen werden auf den Client- und Serversystemen eingesetzt.
	Wie wird sichergestellt, dass nicht mehr benötigte bzw. defekte Datenträger ordnungsgemäß entsorgt werden?	Die anfallenden Datenträger werden zentral durch die IT-Abteilung entsorgt. Funktionsfähige Datenträger werden entsprechend geeigneter Methoden sicher gelöscht. (z.B. mehrfaches Überschreiben) Nicht funktionsfähige Datenträger werden physikalisch vernichtet.

1.7	**Wiederherstellbarkeit**	
	Welche organisatorischen und technischen Maßnahmen werden getroffen, um auch im Schadensfall die Verfügbarkeit von Daten und Systemen schnellstmöglich zu gewährleisten? (rasche Wiederherstellbarkeit nach Art. 32 Abs.1 lit.c DSGVO)	Die Server- und Stromversorgungssysteme der Verarbeitungsanlage sind redundant ausgelegt, um einem Ausfall vorzubeugen. Kundendaten, die in der Cloud vorgehalten werden, sind mit einer Sicherung, die georedundant vorgehalten wird, wiederherzustellen.
1.8	**Auftragskontrolle**	
	Wie stellt der Auftraggeber die ordnungsgemäße Weitergabe von personenbezogenen Daten sicher?	Es werden nur personenbezogene Daten gemäß der Weisung verarbeitet. Ein Subunternehmer wird in gleicher Weise zur Einhaltung und Erfüllung des Datenschutzes verpflichtet.

Für den Auftragnehmer:

Kiel, den 23.01.2023

Ort, Datum

_____

Hauke Lamb

Geschäftsführer

TRASER Software GmbH
Christianspries 4
24159 Kiel
+49 431 - 221394 11
info@traser-software.de