

## Vertrag zur Auftragsverarbeitung

gemäß Art. 28 DS-GVO.



### Restricted – Eingeschränkt

Limited disclosure, restricted to the community.

Recipients may share restricted information with peers and partner organizations, but not via publicly accessible channels. This information may be circulated widely within a particular community. Restricted information may not be released outside of the community.

If you have questions regarding information classification, please contact: [security@bare.id](mailto:security@bare.id)

Zwischen dem/der

- Verantwortlicher - nachstehend Auftraggeber genannt -

und der

**Bare.ID GmbH**

Kirchgasse 6, 65185 Wiesbaden

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt  
wird der folgende

Vertrag zur Auftragsverarbeitung  
gemäß Art. 28 DS-GVO geschlossen:

- Klassifizierung: Eingeschränkt -

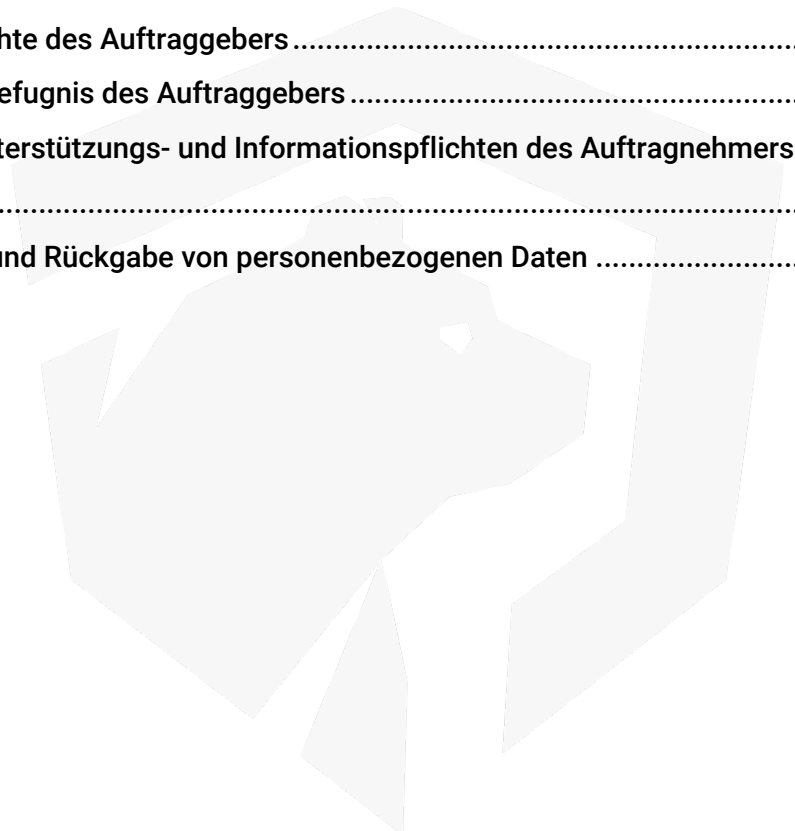
2/12

<b>Kontakt</b>		<b>Geschäftssitz</b>	<b>Geschäftsführer</b>	Elmar Eperiesi-Beck (CEO)	<b>Bank</b>	Wiesbadener Volksbank eG
<b>Telefon</b>	+49 611 945 735 - 0	Bare.ID GmbH		Bastian Ike (CTO)		Schillerplatz 4   65185 Wiesbaden
<b>Fax</b>	+49 611 945 735 - 10	Kirchgasse 6		Kian T. Gould	<b>IBAN</b>	DE15 5109 0000 0005 2908 05
<b>Mail</b>	info@bare.id	65185 Wiesbaden	<b>Registergericht</b>	Wiesbaden B HRB 33190	<b>BIC/SWIFT</b>	WIBADE5W
<b>Web</b>	www.bare.id	Deutschland	<b>USt-IdNr</b>	DE349840819	<b>Land</b>	Deutschland

## Inhaltsverzeichnis

---

1. Gegenstand und Dauer des Vertrags .....	4
2. Konkretisierung des Vertragsinhalts.....	4
3. Technisch-organisatorische Maßnahmen .....	5
4. Rechte von betroffenen Personen.....	6
5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers.....	6
6. Unterauftragsverhältnisse.....	7
7. Internationale Datentransfers .....	9
8. Kontrollrechte des Auftraggebers.....	9
9. Weisungsbefugnis des Auftraggebers .....	10
10. Weitere Unterstützungs- und Informationspflichten des Auftragnehmers .....	10
11. Haftung .....	10
12. Löschung und Rückgabe von personenbezogenen Daten .....	11



## 1. Gegenstand und Dauer des Vertrags

### (1) Gegenstand

Der Gegenstand des Vertrags ergibt sich aus den „Bedingungen für den Betrieb von Bare.ID als Software as a Service“, auf die hier verwiesen wird (im Folgenden Leistungsvereinbarung).

### (2) Dauer

Die Dauer dieses Vertrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

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

(4) 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.

## 2. Konkretisierung des Vertragsinhalts

### (1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind in der Leistungsvereinbarung konkret beschrieben

### (2) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)

- **Personenstammdaten**  
Name und Vorname, Anrede
- **Kommunikationsdaten**  
E-Mail-Adresse und optional: Mobilfunknummer, IP-Adresse bei Zugriffen, öffentlich verfügbare Endgeräte Information
- **Organisationszugehörigkeiten**  
Beliebige optionale Attribute, die die Person in ihrer Organisation klassifizieren wie zum Beispiel Standorte, Teams, Abteilungen, Büro, Hierarchien, Gruppen und

- Klassifizierung: Eingeschränkt -

4/12

<b>Kontakt</b>	<b>Geschäftssitz</b>	<b>Geschäftsführer</b>	Elmar Eperiesi-Beck (CEO)	<b>Bank</b>	Wiesbadener Volksbank eG	
<b>Telefon</b>	+49 611 945 735 - 0	Bare.ID GmbH	Bastian Ike (CTO)		Schillerplatz 4   65185 Wiesbaden	
<b>Fax</b>	+49 611 945 735 - 10	Kirchgasse 6	Kian T. Gould	<b>IBAN</b>	DE15 5109 0000 0005 2908 05	
<b>Mail</b>	info@bare.id	65185 Wiesbaden	<b>Registriergericht</b>	Wiesbaden B HRB 33190	<b>BIC/SWIFT</b>	WIBADE5W
<b>Web</b>	www.bare.id	Deutschland	<b>USt-IdNr</b>	DE349840819	<b>Land</b>	Deutschland

ähnliches, sollten diese zur Autoritätsentscheidung benötigt und über entsprechende Schnittstellen übermittelt werden.

- **Autorisierungsinformationen**  
Login-Name, Passwort-Hash inkl. Historie, weitere Login-Faktoren sowie Zuordnungen zu Berechtigungen, Rollen und Gruppen
- **Historie**  
über Login-Vorgänge, Zugriffsberechtigungen auf Applikationen, Fehlerhafte Logins und ähnliches

### (3) **Kategorien betroffener Personen**

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

## 3. **Technisch-organisatorische Maßnahmen**

- (1) Der Auftragnehmer ergreift in seinem Verantwortungsbereich alle erforderlichen technisch-organisatorischen Maßnahmen gem. Art. 32 DS-GVO zum Schutz der personenbezogenen Daten und übergibt dem Auftraggeber die Dokumentation zur Prüfung [Anhang 1]. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Vertrags.
- (2) Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.
- (3) 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.

## 4. Rechte von betroffenen Personen

- (1) 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.
- (2) 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. Diesbezüglich ist II. Serviceparameter der Leistungsvereinbarung zu beachten.

## 5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

- (1) Der Auftragnehmer hat, zusätzlich zu der Einhaltung der Regelungen dieses Vertrags, eigene gesetzliche Pflichten gemäß der DS-GVO; 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 DS-GVO. 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

Informationensersuchen 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 nach Ziffer 8 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 DS-GVO nachkommen kann. Er fertigt über den gesamten Vorgang eine Dokumentation an, die er dem Auftraggeber für weitere Maßnahmen zur Verfügung stellt. Er trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.
  - 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 relevante 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.
- (2) Dieser Vertrag entbindet den Auftragnehmer nicht von der Einhaltung anderer Vorgaben der DS-GVO.

## 6. Unterauftragsverhältnisse

- (1) 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. Telekommunikationsleistungen, Post-/Transportdienstleistungen, Reinigungsleistungen 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 erbracht werden.

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.

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

Der Auftraggeber stimmt der Beauftragung der in Anhang 2 bezeichneten Unterauftragnehmer sowie dem Einsatz verbundener Unternehmen im Konzern (aktuell AOE GmbH, Omnevo GmbH am gleichen Geschäftssitz wie die Bare.ID GmbH) als Unterauftragnehmer unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO mit dem Unterauftragnehmer zu.

Die vertragliche Vereinbarung wird dem Auftraggeber auf dessen Verlangen vorgelegt, wobei geschäftliche Klauseln ohne datenschutzrechtlichen Bezug hiervon ausgenommen sind.

Die Auslagerung auf Unterauftragnehmer oder der Wechsel der gemäß Anhang 2 bestehenden Unterauftragnehmers sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber in einer angemessenen Zeit, die 14 Tage nicht unterschreiten darf, vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

- (3) 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.

- (4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR, stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende

Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

- (5) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform); sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

## 7. Internationale Datentransfers

- (1) Jede Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation bedarf einer dokumentierten Weisung des Auftraggebers und bedarf der Einhaltung der Vorgaben zur Übermittlung personenbezogener Daten in Drittländer nach Kapitel V der DS-GVO.

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.

- (2) Soweit der Auftraggeber eine Datenübermittlung an Dritte in ein Drittland anweist, ist er für die Einhaltung von Kapitel V der DS-GVO verantwortlich.

## 8. Kontrollrechte des Auftraggebers

- (1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch einen im Einzelfall zu benennenden 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.
- (2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO 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.
- (3) Der Nachweis der technisch-organisatorischen Maßnahmen zur Einhaltung der besonderen Anforderungen des Datenschutzes allgemein sowie solche, die den Auftrag betreffen, kann erfolgen durch
  - a) die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
  - b) die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;

- c) aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- d) eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz bzw. ISO 2700x).

## 9. Weisungsbefugnis des Auftraggebers

- (1) 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.
- (2) 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.

## 10. Weitere Unterstützungs- und Informationspflichten des Auftragnehmers

- (1) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person nach Art. 82 DSGVO unterstützt der Auftragnehmer den Auftraggeber in einem angemessenen Umfang. Im Falle einer Inanspruchnahme des Auftragnehmers durch eine betroffene Person nach Art. 82 DSGVO hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren.
- (2) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren, durch Verlangen nach Offenlegung im Zusammenhang mit gerichtlichen Verfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang verantwortlichen Stellen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber liegen.

## 11. Haftung

- (1) Der Auftragnehmer haftet gegenüber dem Auftraggeber nach Maßgabe der gesetzlichen Bestimmungen. Der Auftragnehmer haftet dem Auftraggeber für Verstöße der

Unterauftragnehmer gegen datenschutzrechtliche Bestimmungen wie für eigenes Verschulden.

- (2) Sofern Dritte Ansprüche gegen den Auftraggeber wegen der Verletzung datenschutzrechtlicher Bestimmungen geltend machen, die allein auf einen Verstoß des Auftragnehmers oder seiner Unterauftragnehmer gegen datenschutzrechtliche Bestimmungen oder gegen die Bestimmungen des Vertrags basieren, übernimmt der Auftragnehmer auf eigene Kosten die Verteidigung des Rechtsstreits und stellt den Auftraggeber von sämtlichen Ansprüchen sowie den angemessenen Kosten der Rechtsverfolgung frei. Der Verantwortliche wird den Auftragnehmer unverzüglich über die entsprechenden Anspruchsschreiben Dritter informieren und – soweit möglich – dem Auftragnehmer die Befugnisse einräumen, sich selbstständig gegen die Ansprüche zu verteidigen.

## 12. Löschung und Rückgabe von personenbezogenen Daten

- (1) 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.
- (2) 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.

Ort, Datum:

Verantwortlicher:

Unterzeichner:

Ort, Datum:

Verarbeiter: Bare.ID GmbH

Unterzeichner:

Stempel / Unterschrift

Stempel / Unterschrift



- Klassifizierung: Eingeschränkt -

12/12

<b>Kontakt</b>	<b>Geschäftssitz</b>	<b>Geschäftsführer</b>	Elmar Eperiesi-Beck (CEO)	<b>Bank</b>	Wiesbadener Volksbank eG
<b>Telefon</b>	Bare.ID GmbH		Bastian Ike (CTO)		Schillerplatz 4   65185 Wiesbaden
<b>Fax</b>	Kirchgasse 6		Kian T. Gould	<b>IBAN</b>	DE15 5109 0000 0005 2908 05
<b>Mail</b>	65185 Wiesbaden	<b>Registergericht</b>	Wiesbaden B HRB 33190	<b>BIC/SWIFT</b>	WIBADE5W
<b>Web</b>	Deutschland	<b>USt-IdNr</b>	DE349840819	<b>Land</b>	Deutschland