Vereinbarung
Auftragsverarbeitung

Vereinbarung über die Auftragsverarbeitung zwischen Kunde nachfolgend „Auftraggeber" genannt und BRUNATA-METRONA GmbH, Max-Planck-Str. 2 in 50354 Hürth, nachfolgend „BRUNATA-METRONA" genannt. Beide Parteien nachfolgend auch als „Vertragspartner" bezeichnet.

Präambel

Im Rahmen der Zusammenarbeit der Vertragsparteien erhält BRUNATA-METRONA Zugriff auf personenbezogene Daten des Auftraggebers. BRUNATA-METRONA ist insoweit zur Vertraulichkeit und Sicherung dieser Daten verpflichtet. Es bedarf darüber hinaus auch einer vertraglichen Vereinbarung über die Verarbeitung dieser personenbezogenen Daten.

1. Gegenstand und Dauer des Vertrages

1.1 Gegenstand dieses Vertrages ist die Regelung und Konkretisierung der datenschutzrechtlichen Rechte und Pflichten der Vertragspartner, die sich aus dem Hauptvertrag und der damit zusammenhängenden Auftragsverarbeitung ergeben.

1.2 Die Dauer dieses Vertrages sowie Kündigungsfristen entsprechen den Regelungen des Hauptvertrages. Mit Beendigung und/oder Kündigung des Hauptvertrages bzw. des letzten hierunter abgeschlossenen Einzelauftrags endet auch dieser Vertrag über die Auftragsverarbeitung automatisch, ohne dass es einer gesonderten Kündigung bedarf.

1.3 Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

1.4 Das Recht, diesen Vertrag ohne die Einhaltung einer Frist (fristlos) außerordentlich zu kündigen, weil auf Grund der Schwere und der Bedeutung einer erfolgten Pflichtverletzung ein Festhalten am Vertrag nicht zumutbar ist, bleibt für beide Parteien unberührt.

2. Art und Zweck der Verarbeitung

Umfang, Art und Zweck der Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch BRUNATA-METRONA für den Auftraggeber ergeben sich aus den zum Zeitpunkt der Unterzeichnung bestehenden Verträgen (Einzelvertrag bzw. Rahmenvertrag) sowie aus den ggf. zukünftig noch zu schließenden Verträgen, soweit sie eine Auftragsverarbeitung i.S.d. Artikels 28 DS-GVO zum Gegenstand haben.

3. Art der personenbezogenen Daten

Gegenstand der Verarbeitung sind folgende Datenkategorien:

[X] Vor- und Nachname	[X] Anrede	[X] Adresse	[X] Nutzer-ID
[X] E-Mail	[X] Anzahl der Personen im Haushalt	[X] Vollmacht	[X] Abrechnungsdaten
[X] Quadratmeter der Wohnung	[X] Lage der Wohnung (Wohnungsnummer und Stockwerk)	[X] Laborbefunde Trinkwasseranalyse	[X] Verbrauchsdaten
[ ] Gebäudebilder	[ ]	[ ]	[ ]

4. Kategorien der betroffenen Personen

Gegenstand der Verarbeitung sind folgende Kategorien:

[X] Eigentümer	[X] Dienstleister	[X] Hausverwalter	[X] Bevollmächtigte
[X] Mieter	[ ]	[ ]	[ ]

BRUNATA-METRONA GmbH ▪ Max-Planck-Str. 2 ▪ 50354 Hürth ▪ Telefon +49 2233 50-0 ▪ Fax +49 2233 50-1169 www.brunata-metrona.de

5. Rechte und Pflichten

5.1 Weisungsrecht

(1) BRUNATA-METRONA und jede der BRUNATA-METRONA unterstellte Person, die Zugang zu personenbezogenen Daten hat, werden diese Daten im Hinblick auf die Zwecke der Verarbeitung, die relevanten Verarbeitungsschritte und die Verwendung ausschließlich auf Weisung des Auftraggebers verarbeiten.

(2) Die Weisungen sind durch den Auftraggeber, einen bestellten Verwalter oder durch eine vom Auftraggeber gesondert benannte Person gegenüber BRUNATA-METRONA in Textform zu erteilen. Die Kontaktdaten der gesondert benannten Personen sind BRUNATA-METRONA mitzuteilen und als dann zu ergänzende Anlage zu dokumentieren.

(3) BRUNATA-METRONA hat das Recht, aber nicht die Pflicht, Weisungen auf eine mögliche Rechtswidrigkeit zu überprüfen. Hiervon abgesehen wird BRUNATA-METRONA den Auftraggeber unverzüglich informieren, falls BRUNATA-METRONA der Auffassung ist, eine Weisung verstoße gegen Datenschutzvorschriften.

5.2 Vertraulichkeitsverpflichtung

(1) BRUNATA-METRONA setzt bei der Durchführung der vertragsgegenständlichen Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit (Verschwiegenheit) verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden.

(2) BRUNATA-METRONA ist darüber hinaus verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse, insbesondere von Betriebsgeheimnissen und Datensicherheitsmaßnahmen des Auftraggebers auch über das Vertragsende hinaus vertraulich zu behandeln.

5.3 Sicherheit der Verarbeitung

(1) BRUNATA-METRONA verpflichtet sich, diejenigen technischen und organisatorischen Maßnahmen zu treffen und während der Vertragslaufzeit aufrechtzuerhalten, die erforderlich sind, um das angemessene Schutzniveau für die personenbezogenen Daten des Auftraggebers zu gewährleisten.

(2) Bei den zu treffenden Maßnahmen handelt es sich um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der jeweilige Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen zu berücksichtigen, siehe hierzu **Anlage 1**. Insoweit ist es BRUNATA-METRONA gestattet, die Maßnahmen anzupassen, wenn und soweit das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten wird und die Änderungen nachvollziehbar dokumentiert werden.

5.4 Unterauftragsverhältnisse

(1) Voraussetzung jeglicher Auslagerung ist eine vertragliche Vereinbarung nach Maßgabe des Art. 28 DS-GVO, in den sämtlichen vorliegenden vertraglichen Regelungen in der Vertragskette auch dem weiteren Unterauftragnehmer auferlegt werden.

(2) Dem Auftraggeber ist bekannt, dass BRUNATA-METRONA zur Erfüllung der vertraglichen Pflichten Unterauftragnehmer zur Vertragserfüllung einsetzt. Hierbei handelt es sich um einen Unterauftragnehmer-Pool, aus dem die jeweiligen Unterauftragnehmer beauftragt werden.

Insoweit wird bereits jetzt vereinbart, dass im Falle der Betreuung vor Ort durch eine Niederlassung die Ableser und Monteure, die notwendig sind, um die Geräte von METRONA zu montieren, abzulesen bzw. zu warten oder die Trinkwasseranalyse durchzuführen als Unterauftragnehmer genehmigt werden.

Weitere Unterauftragnehmer sind: Die RheinEnergie AG in Köln, die q.beyond AG in Köln, die NetCologne IT Services GmbH in Köln, die synavision GmbH in Bielefeld, die Noumena Digital AG in Baar (CH), die bimanu Cloud Solutions GmbH in Neuss, DATASEC information factory GmbH in Siegen und die salesforce.com EMEA Limited in London als weitere Unterauftragnehmer für IT-Leistungen.

Die weitere Auslagerung durch den Unterauftragnehmer und der Wechsel der bei Vertragsschluss bestehenden weiteren Unterauftragsnehmer ist zulässig, soweit der Auftraggeber nicht gegenüber BRUNATA-METRONA schriftlich oder in Textform Einspruch gegen die geplante weitere Auslagerung erhebt.

5.5 Unterstützung und Meldung

(1) Sofern BRUNATA-METRONA eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet sie diese dem Auftraggeber unverzüglich.

(2) BRUNATA-METRONA unterstützt den Auftraggeber bei der Erfüllung seiner Informationspflichten gegenüber der jeweils zuständigen Aufsichtsbehörde bzw. diejenigen, die von einer Verletzung des Schutzes personenbezogener Daten betroffen sind.

(3) Ist der Auftraggeber auf Grund geltender Datenschutzgesetze gegenüber einer betroffenen Person verpflichtet, Auskünfte zur Erhebung, Verarbeitung oder Nutzung von Daten dieser Person zu geben, wird BRUNATA-METRONA den Auftraggeber dabei unterstützen, diese Informationen bereitzustellen, vorausgesetzt der Auftraggeber hat BRUNATA-METRONA hierzu schriftlich oder in Textform aufgefordert.

5.6 Weitergehende Unterstützung des Auftraggebers

(1) BRUNATA-METRONA wird den Auftraggeber bei der Einhaltung der Pflichten im Zusammenhang mit der Sicherheit personenbezogener Daten, den Meldepflichten bei Datenpannen gegenüber den Aufsichtsbehörden und den Betroffenen sowie bei der Erstellung und Pflege von Datenschutz-Folgeabschätzungen und den vorherigen Konsultationen unterstützen.

(2) Sofern die Unterstützung über die gesetzlich vorgeschriebene Unterstützung nach Punkt 5.5 hinausgeht, kann BRUNATA-METRONA eine Vergütung beanspruchen, die vorab zwischen den Vertragspartnern zu vereinbaren wäre.

5.7 Datenrückgabe

(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 mit Beendigung des Hauptvertrages – wird BRUNATA-METRONA nach Wahl des Auftraggebers die personenbezogenen Daten löschen oder zurückgeben.

(3) Dokumentationen und Informationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen oder gesetzlichen Aufbewahrungspflichten unterliegen, sind hiervon ausgenommen.

5.8 Nachweis- und Kontrollrechte

(1) BRUNATA-METRONA wird dem Auftraggeber alle erforderlichen Informationen zur Verfügung stellen, um nachzuweisen, dass BRUNATA-METRONA den Verpflichtungen als Auftragsverarbeiter nachkommt.

(2) Hierzu zählt auch das Recht, in Absprache mit BRUNATA-METRONA Überprüfungen und Inspektionen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen.

5.9 Datenschutzbeauftragte(r)

BRUNATA-METRONA ist zur Bestellung eines/r Datenschutzbeauftragten verpflichtet.

Der Auftraggeber erreicht diese/n unter:
BRUNATA-METRONA GmbH, Datenschutzbeauftragte/r, Max-Planck-Str. 2 in 50354 Hürth, Tel.: 02233-50- 0,
E-Mail: datenschutz@brunata-huerth.de.

6. Haftung

6.1 BRUNATA-METRONA haftet im Innenverhältnis zum Auftraggeber für den durch eine Verarbeitung verursachten Schaden nur, wenn BRUNATA-METRONA

(1) den speziell durch die DS-GVO auferlegten Pflichten für Auftragsverarbeiter nicht nachgekommen ist oder

(2) unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des Auftraggebers oder gegen diese Anweisungen gehandelt hat.

6.2 Weitergehende Haftungsansprüche nach den allgemeinen Gesetzen bleiben unberührt.

Hierzu zählt auch die Haftung für Schäden der Vertragspartner, ihrer gesetzlichen Vertreter und Erfüllungsgehilfen, die vorsätzlich oder grob fahrlässig verursacht werden oder die aus der schuldhaften Verletzung des Lebens, des Körpers oder der Gesundheit resultieren.

7. Schlussbestimmungen

7.1 Im Fall von Widersprüchen zwischen diesem Vertrag und sonstigen Vereinbarungen zwischen den Parteien, insbesondere dem Hauptvertrag, gehen die Regelungen dieses Vertrags vor.

7.2 Nebenabreden, Änderungen und Ergänzungen dieses Vertrages bedürfen der Textform. Dies gilt auch für die Änderung dieser Schriftformvereinbarung.

7.3 Es gelten die gesetzlichen Bestimmungen der Datenschutz-Grundverordnung, im Übrigen das Recht der Bundesrepublik Deutschland.

7.4 Gerichtsstand ist der Sitz von BRUNATA-METRONA.

7.5 Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden, so bleiben die übrigen Bestimmungen hiervon unberührt. Die Parteien verpflichten sich, anstelle der unwirksamen Regelungen eine solche gesetzlich zulässige Regelung zu treffen, die dem Zweck der unwirksamen Regelungen am nächsten kommt.

Anlage 1 – Technische und organisatorische Maßnahmen

Gemäß Art. 32 DS-GVO sind geeignete technisch-organisatorische Maßnahmen unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen seitens des Verantwortlichen und der Auftragsverarbeiter zu treffen. BRUNATA-METRONA setzt die Anforderungen in seinem Einflussbereich in Bezug auf diese Vereinbarung wie folgt um:

1. Pseudonymisierung und Verschlüsselung

Anforderung	Bewertung für die Auftragsverarbeitung
Unter Pseudonymisierung versteht man das Ersetzen von Identifikationsmerkmalen mit einer für das Identifikationsmerkmal eindeutigen Kennung, dem Pseudonym. Eine Re-Identifikation ist prinzipiell möglich, sobald die Abbildungstabelle zwischen Identifikationsmerkmal und Pseudonym herangezogen wird. Zielsetzung der Pseudonymisierung ist, das Risiko für den Betroffenen bei der Verarbeitung seiner personenbezogenen Daten zu senken. Dies resultiert daraus, dass beispielsweise bei einem unbefugten Zugriff auf pseudonymisierte Daten mittels eines Hacking-Angriffs das Pseudonym ohne Mitwirkung des Verantwortlichen (von der nicht auszugehen ist) einer konkreten identifizierbaren Person eher schwerer zuzuordnen ist.	Eine Pseudonymisierung findet z. B. nach mehrjährigem Nutzerauszug aus der abzurechenden Liegenschaft statt. Die betroffenen Daten sind danach nicht mehr personenbezogen.
Der Einsatz von kryptographischen Verfahren gehört zu den Standardmaßnahmen des technischen Datenschutzes, da damit wirksam die Vertraulichkeit und Integrität der personenbezogenen Daten geschützt werden können.	Eine Verschlüsselung der E-Mail-Übertragung erfolgt per TLS (Transport Layer Security). Die Datenbanken auf den eingesetzten mobilen Endgeräten sind verschlüsselt. Ebenso die Datenübertragung aus der Zentrale an die mobilen Endgeräte und zurück erfolgt verschlüsselt und nach dem aktuellen Stand der Technik.

2. Verfahren zur Gewährleistung von Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung

2.1 Zugangs-, Zutritts- und Zugriffskontrolle sowie Eingabekontrolle

Anforderung

Maßnahmen, damit Unbefugten der Zutritt zu den Datenverarbeitungsanlagen verwehrt wird, mit denen personenbezogene Daten verarbeitet werden. Es muss zudem verhindert werden, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können oder von Unbefugten der physische Zugang zu Einrichtungen oder Räumlichkeiten ermöglicht wird, in denen IT-Systeme betrieben und genutzt werden (z. B. Rechenzentren oder Arbeitsräume); Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können; Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind.

Umsetzung

[X]	1.1.1	Rechner verfügen über individuelle, personenbezogene Benutzerkennungen	[X] 1.1.13	Server verfügen über individuelle Benutzerkennungen
[X]	1.1.2	Zwei-Faktor-Authentisierung	[X] 1.1.14	Das Firmennetzwerk ist durch eine Firewall geschützt
[X]	1.1.3	Passwortrichtlinie	[X] 1.1.15	Datentrennung innerhalb des Firmennetzwerkes
[X]	1.1.4	Der Zugang zum System wird gesperrt bei fehlerhafter Eingabe des Passwortes nach 5 Versuchen	[X] 1.1.16	Nur vereinzelte mit besonderen Aufgaben versehene Mitarbeiter haben Administrationsrechte
[X]	1.1.5	Virenscanner auf allen Client-Computern	[X] 1.1.17	Es besteht eine Zutrittsregelung für RZ- und Serverräume

BRUNATA-METRONA GmbH ▪ Max-Planck-Str. 2 ▪ 50354 Hürth ▪ Telefon +49 2233 50-0 ▪ Fax +49 2233 50-1169 www.brunata-metrona.de

X	1.1.6	Es besteht eine Zutrittsüberwachung spezieller Arbeitsräume	☐	1.1.18	Der Gebäudezugang über die Tiefgarage ist videoüberwacht
X	1.1.7	Die Gebäude sind mit einer Alarm- und Schließanlage gesichert	X	1.1.19	Die Gebäude werden von einem Wachdienst außerhalb der regulären Arbeitszeit gesichert
X	1.1.8	Manuelle Schließanlage der Eingangstüren	X	1.1.20	Chipkarten für Schließanlage der Eingangstüren
X	1.1.9	Die Nutzung der Schließanlage ist dokumentiert	X	1.1.21	Der Zutritt und Aufenthalt von Besuchern erfolgt in Begleitung von Firmenpersonal
X	1.1.10	Der Zutritt von Besuchern zum Gebäude wird dokumentiert	X	1.1.22	Der Zutritt von Reinigungs- und Wartungspersonal zum Gebäude ist geregelt
X	1.1.11	Automatisierte Sperrung bei Inaktivität des PCs	X	1.1.23	Administratorrechte sind definiert
X	1.1.12	Der Entzug von Gebäudezutrittsberechtigungen ist geregelt und dokumentiert	X	1.1.24	Die Rechenzentren sind alarmgesichert

2.2 Belastbarkeit der Systeme

Anforderung

Der Begriff der Belastbarkeit („Resilienz“) beschreibt die Fähigkeit des Unternehmens, auch bei Störungen und Eingriffen möglichst unbeschadet weiter existieren zu können. Hierzu zählen z. B. die üblichen IT-Schutzmaßnahmen.

Umsetzung

X	1.2.1	Datenträger und Datenspeicher werden zugriffssicher aufbewahrt	X	1.2.18	Zugang zu Storage-Lösungen wird für Unbefugte physisch verhindert
X	1.2.2	Datenträger und Datenspeicher werden professionell entsorgt/vernichtet	X	1.2.19	Datenträger und Datenspeicher unterliegen einem Aufbewahrungs- und Löschkonzept
X	1.2.3	Storage-Systeme werden räumlich abgeschirmt	X	1.2.20	Dokumentierter und sicherer Lebenszyklus von Datenträgern geregelt
X	1.2.4	Integrität und Manipulationssicherheit bei Storage-Systemen	X	1.2.21	Belastbarkeit der Storage-Systeme ist durch Redundanz und Performancetests gewährleistet
X	1.2.5	Mandantenfähigkeit bei den Storage-Systemen	X	1.2.22	Rollen- und Berechtigungskonzepte
X	1.2.6	Auswertbarkeit über Zugriffsprotokolle möglich	☐	1.2.23	Getrennte Arten von Storage-Administration vorhanden
☐	1.2.7	Einsatz und Implementierung von Sandbox-Verfahren	X	1.2.24	Ansprechpartner genannt, geschult und Verarbeitungsprozesse definiert
X	1.2.8	Datensicherheitskonzepte vorhanden	X	1.2.25	Incident Management vorhanden
X	1.2.9	Kommunikationsregelung bei IT-Ausfällen	X	1.2.26	Revisionsfestigkeit von Daten gewährleistet
X	1.2.10	Regelmäßige und unregelmäßige Datenschutz- und Datensicherheitskontrollen	X	1.2.27	Aktuelle Backuplösungen zur Wiederherstellbarkeit
X	1.2.11	Kurze Wiederanlaufzeit des Rechenzentrums durch Redundanz abgesichert	X	1.2.28	Gebäude und Einrichtungen sind je nach Kritikalität gemäß den technischen Standards vor Zerstörung (z. B. Brand) geschützt
X	1.2.12	Es bestehen Verträge für die Wartung von IT-Systemen durch externe Unternehmen	X	1.2.29	Datensicherungsrichtlinie vorhanden
X	1.2.13	Gebäude und Einrichtungen halten je nach Kritikalität gemäß den technischen Standards eine angemessene Gewährleistung und Absicherung der Energieversorgung vor	X	1.2.30	Patch Management vorhanden
X	1.2.14	Verschlüsselter Transport von Daten vorhanden	☐	1.2.31	Datenmigrationsvorgehen definiert
X	1.2.15	Sicherheitstresore für Schutz von Datenträger vorhanden	X	1.2.32	Redundanz-Systeme und Clustering-Systeme vorhanden
X	1.2.16	Prüfung der Empfänger (NDA, Compliance)	X	1.2.33	Aktualisierungsvorgehen für Einsatz Schutzsoftware vorhanden
☐	1.2.17	Es werden Log-Files für die Nachvollziehbarkeit der Löschung/Änderung von Daten des Auftraggebers erstellt	X	1.2.34	Datenschutzpannen-Konzept vorhanden

3. Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen

Anforderung			
Maßnahmen, die gewährleisten, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können.			
Umsetzung			
[X]	2.1.1 Datenbackupkonzept vorhanden	[X]	2.1.6 Redundanzsysteme vorhanden und Ablaufvorgehen definiert
[X]	2.1.2 Kommunikationsabsprache bei IT-Ausfällen vorhanden	[X]	2.1.7 Incident Management vorhanden
[X]	2.1.3 Regelmäßige und unregelmäßige Datenschutz- und Datensicherheitskontrollen	[X]	2.1.8 Dokumentation der Mandantentrennung vorhanden
[X]	2.1.4 Physische oder (programm-) technische Trennung von Daten (Mandantentrennung).	[X]	2.1.9 Unterschiedliche Zugriffsrechte erforderlich (und dokumentiert), um die Mandantentrennung zu gewährleisten
[X]	2.1.5 Nutzung unterschiedlicher (Datenbank-) Dateien (Datei-Separation)	[X]	2.1.10 Trennung von Test- und Produktivdaten gewährleistet

4. Verfahren, die der regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung dienen

Anforderung	**Bewertung für die Auftragsverarbeitung**
Informationssicherheit ist (auch) ein Prozess, d. h. Sicherheitsprodukte alleine sind nicht ausreichend zur Gewährleistung eines angemessenen Schutzniveaus und gehört seit langem zum üblichen Verständnis beim Schutz von Informationen (hier: personenbezogene Daten). Auch beim Schutz personenbezogener Daten muss ein geeigneter prozessorientierter Ansatz verfolgt werden, der sich beispielsweise auch in (bereits bestehenden) Informationssicherheitsmanagementsystemen wiederfindet, die um den technischen Datenschutz erweitert werden können.	BRUNATA-METRONA hat fest definierte Zyklen, innerhalb derer die Anforderungen an die Datensicherheit überprüft werden. Hierbei wird auch das o. g. Schutzniveau stets erneut auf den Prüfstand gestellt. Turnusmäßig findet eine Überarbeitung einmal jährlich anlassunabhängig statt.

5. Verfahren zur Gewährleistung, dass Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten

Anforderung	**Bewertung für die Auftragsverarbeitung**
Maßnahmen, die gewährleisten, dass personenbezogene Daten vom Auftraggeber nur gemäß dessen Weisungen verarbeitet werden. Beschäftigt der Partner einen Unterauftragnehmer, so muss er diesen in gleicher Weise zur Erfüllung der Weisungen und zur Einhaltung des Datenschutzes verpflichten.	Alle Mitarbeiter sind auf den Datenschutz und auf die Einhaltung der Handlungsanweisungen verpflichtet, wie personenbezogene oder personenbeziehbare Daten behandelt werden.

BRUNATA-METRONA GmbH ▪ Max-Planck-Str. 2 ▪ 50354 Hürth ▪ Telefon +49 2233 50-0 ▪ Fax +49 2233 50-1169 www.brunata-metrona.de