Vertrag zur Auftragsverarbeitung personenbezogener Daten gemäß BDSG und DSGVO im Rahmen der Nutzung der brytes empathy engine

zwischen

dem Nutzungslizenznehmer der brytes empathy engine

im Folgenden „Auftraggeber“ genannt

und

synaigy GmbH
Im Mediapark 5
50670 Köln
Deutschland
Ansprechpartner: Joubin Rahimi (joubin.rahimi@synaigy.com)
im Folgenden „Auftragnehmer“ genannt

im Folgenden gemeinsam „Geschäftspartner“, „Partner“ oder „Parteien“ genannt.

synaigy

Versionskontrolle:

Version	Änderungen	Bearbeiter	Datum
V00.000	Erstellung Erstversion		

Inhaltsverzeichnis

_Anschrift
synaigy GmbH
Im Mediapark 5, D-50670 Köln
T +49 221 9 73 43-0
info@synaigy.com

_Bankverbindung
Commerzbank Köln
IBAN DE15 3704 0044 0124 7253 00
BIC COBADEFF370

_Gerichtsstand
GmbH Sitz: Köln
Registergericht Köln
HRB: 72797
USt-IdNr.: DE277514575

_Geschäftsführer
Joubin Rahimi

1 Allgemeines

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers i.S.d. Art. 4 Nr. 8 und Art. 28 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (DSGVO). Dieser Vertrag regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung von personenbezogenen Daten.

(2) Sofern in diesem Vertrag der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird die Definition der „Verarbeitung“ i.S.d. Art. 4 Nr. 2 DSGVO zugrunde gelegt.

2 Gegenstand des Auftrags

Der Gegenstand der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen sind in **Anlage 1** zu diesem Vertrag festgelegt.

3 Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber ist Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer. Dem Auftragnehmer steht nach Ziff. 4 Abs. 3 das Recht zu, den Auftraggeber darauf hinzuweisen, wenn eine seiner Meinung nach rechtlich unzulässige Datenverarbeitung Gegenstand des Auftrags und/oder einer Weisung ist.

(2) Der Auftraggeber ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte gegenüber dem Auftragnehmer geltend machen.

(3) Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen. Weisungen müssen in Textform (z.B. E-Mail) erfolgen.

(4) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers beim Auftragnehmer entstehen, bleiben unberührt.

(5) Der Auftraggeber kann weisungsberechtigte Personen benennen. Sofern weisungsberechtigte Personen benannt werden sollen, werden diese in der **Anlage 1** benannt. Für den Fall, dass sich die weisungsberechtigten Personen beim Auftraggeber ändern, wird der Auftraggeber dies dem Auftragnehmer in Textform mitteilen.

(6) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.

(7) Für den Fall, dass eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DSGVO oder einer sonstigen, für den Auftraggeber geltenden gesetzlichen Meldepflicht besteht, ist der Auftraggeber für deren Einhaltung verantwortlich.

4 Allgemeine Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und/oder unter Einhaltung der ggf. vom Auftraggeber erteilten ergänzenden Weisungen. Ausgenommen hiervon sind gesetzliche Regelungen, die den Auftragnehmer ggf. zu einer anderweitigen Verarbeitung verpflichten. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Zweck, Art und Umfang der Datenverarbeitung richten sich ansonsten ausschließlich nach diesem Vertrag und/oder den Weisungen des Auftraggebers. Eine hiervon

abweichende Verarbeitung von Daten ist dem Auftragnehmer untersagt, es sei denn, dass der Auftraggeber dieser schriftlich zugestimmt hat.

(2) Der Auftragnehmer wird die Datenverarbeitung im Auftrag grundsätzlich in Mitgliedsstaaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) durchführen. Dem Auftragnehmer ist eine Datenverarbeitung auch außerhalb von EU oder EWR erlaubt, wenn entsprechende Unterauftragnehmer im Drittland unter Einhaltung der Voraussetzungen von Ziff. 9 eingesetzt werden und die Voraussetzungen der Art. 44-48 DSGVO erfüllt sind bzw. eine Ausnahme i.S.d. Art. 49 DSGVO vorliegt.

(3) Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Sofern der Auftragnehmer darlegen kann, dass eine Verarbeitung nach Weisung des Auftraggebers zu einer Haftung des Auftragnehmers nach Art. 82 DSGVO führen kann, steht dem Auftragnehmer das Recht frei, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Parteien auszusetzen.

(4) Der Auftragnehmer kann dem Auftraggeber die Person(en) benennen, die zum Empfang von Weisungen des Auftraggebers berechtigt sind. Sofern weisungsempfangsberechtigte Personen benannt werden sollen, werden diese in der **Anlage 1** benannt. Für den Fall, dass sich die weisungsempfangsberechtigten Personen beim Auftragnehmer ändern, wird der Auftragnehmer dies dem Auftraggeber in Textform mitteilen.

5 Datenschutzbeauftragter des Auftragnehmers

(1) Der Auftragnehmer bestätigt, dass er einen Datenschutzbeauftragten nach Art. 37 DSGVO benannt hat. Der Auftragnehmer trägt Sorge dafür, dass der Datenschutzbeauftragte über die erforderliche Qualifikation und das erforderliche Fachwissen verfügt.

Der Datenschutzbeauftragte zum Zeitpunkt des Vertragsschlusses ist

Hanno Kortmann

Tel.: +49 221 97343-277

E-Mail: datenschutz@synaigy.com

(2) Bei Änderung des Datenschutzbeauftragten wird der Auftragnehmer den Auftraggeber unverzüglich informieren.

6 Meldepflichten des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Auftraggebers, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist, unverzüglich mitzuteilen. Gleiches gilt für jede Verletzung des Schutzes personenbezogener Daten, die der Auftragnehmer im Auftrag des Auftraggebers verarbeitet.

(2) Ferner wird der Auftragnehmer den Auftraggeber unverzüglich darüber informieren, wenn eine Aufsichtsbehörde nach Art. 58 DSGVO gegenüber dem Auftragnehmer tätig wird und dies auch eine Kontrolle der Verarbeitung, die der Auftragnehmer im Auftrag des Auftraggebers erbringt, betreffen kann.

(3) Dem Auftragnehmer ist bekannt, dass für den Auftraggeber eine Meldepflicht nach Art. 33, 34 DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der Auftragnehmer wird den Auftraggeber bei der Umsetzung der

Meldepflichten unterstützen. Der Auftragnehmer wird dem Auftraggeber insbesondere jeden unbefugten Zugriff auf personenbezogene Daten, die im Auftrag des Auftraggebers verarbeitet werden, unverzüglich ab Kenntnis des Zugriffs mitteilen. Die Meldung des Auftragnehmers an den Auftraggeber muss insbesondere folgende Informationen beinhalten:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener 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;
- eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

7 Mitwirkungspflichten des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nach Art. 12-23 DSGVO. Es gelten die Regelungen von Ziff. 12 dieses Vertrages.

(2) Der Auftragnehmer wirkt an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten durch den Auftraggeber mit. Er hat dem Auftraggeber die insoweit jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

(3) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Art. 32-36 DSGVO genannten Pflichten.

8 Regelung zu mobilen Arbeitsplätzen

(1) Der Auftragnehmer darf seinen Beschäftigten, die mit der Verarbeitung von personenbezogenen Daten für den Auftraggeber beauftragt sind, die Verarbeitung von personenbezogenen Daten an mobilen Arbeitsplätzen außerhalb der Geschäftsräume des Auftragnehmers erlauben.

(2) Der Auftragnehmer hat sicherzustellen, dass die Einhaltung der vertraglich vereinbarten technischen und organisatorischen Maßnahmen auch bei der Nutzung von mobilen Arbeitsplätzen der Beschäftigten des Auftragnehmers gewährleistet ist. Abweichungen von einzelnen vertraglich vereinbarten technischen und organisatorischen Maßnahmen sind vorab mit dem Auftraggeber abzustimmen und von diesem in Textform zu genehmigen.

(3) Der Auftragnehmer trägt insbesondere Sorge dafür, dass bei einer Verarbeitung von personenbezogenen Daten an mobilen Arbeitsplätzen die Speicherorte so konfiguriert werden, dass eine lokale Speicherung von Daten auf IT-Systemen ausgeschlossen ist. Sollte dies nicht möglich sein, hat der Auftragnehmer Sorge dafür zu tragen, dass die lokale Speicherung ausschließlich verschlüsselt erfolgt und andere am Ort des jeweiligen mobilen Arbeitsplatzes befindliche Personen keinen Zugriff auf diese Daten erhalten.

(4) Der Auftragnehmer ist verpflichtet, Sorge dafür zu tragen, dass eine wirksame Kontrolle der Verarbeitung personenbezogener Daten im Auftrag an mobilen Arbeitsplätzen durch den Auftraggeber möglich ist.

(5) Sofern auch bei Unterauftragnehmern Beschäftigte an mobilen Arbeitsplätzen eingesetzt werden sollen, gelten die Regelungen der Absätze 1 bis 4 entsprechend.

9 Kontrollbefugnisse

(1) Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen und/oder

die Einhaltung der Weisungen des Auftraggebers durch den Auftragnehmer im erforderlichen Umfang zu kontrollieren.

(2) Der Auftragnehmer ist dem Auftraggeber gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle i.S.d. Absatzes 1 erforderlich ist.

(3) Der Auftraggeber kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Absatzes 1 in der Betriebsstätte des Auftragnehmers zu den jeweils üblichen Geschäftszeiten vornehmen. Der Auftraggeber wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, um die Betriebsabläufe des Auftragnehmers durch die Kontrollen nicht unverhältnismäßig zu stören. Die Parteien gehen davon aus, dass eine Kontrolle höchstens einmal jährlich erforderlich ist. Weitere Prüfungen sind vom Auftraggeber unter Angabe des Anlasses zu begründen. Im Falle von Vor-Ort-Kontrollen wird der Auftraggeber dem Auftragnehmer die entstehenden Aufwände inkl. der Personalkosten für die Betreuung und Begleitung der Kontrollpersonen vor Ort in angemessenen Umfang ersetzen. Die Grundlagen der Kostenberechnung werden dem Auftraggeber vom Auftragnehmer vor Durchführung der Kontrolle mitgeteilt.

(4) Nach Wahl des Auftragnehmers kann der Nachweis der Einhaltung der technischen und organisatorischen Maßnahmen anstatt einer Vor-Ort-Kontrolle auch durch die Vorlage eines geeigneten, aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren oder Qualitätsauditoren) oder einer geeigneten Zertifizierung erbracht werden, wenn der Prüfungsbericht es dem Auftraggeber in angemessener Weise ermöglicht, sich von der Einhaltung der technischen und organisatorischen Maßnahmen gemäß Anlage 3 zu diesem Vertrag zu überzeugen. Sollte der Auftraggeber begründete Zweifel an der Eignung des Prüfdokuments i.S.d. Satzes 1 haben, kann eine Vor-Ort-Kontrolle durch den Auftraggeber erfolgen. Dem Auftraggeber ist bekannt, dass eine Vor-Ort-Kontrolle in Rechenzentren nicht oder nur in begründeten Ausnahmefällen möglich ist.

(5) Der Auftragnehmer ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber i.S.d. Art. 58 DSGVO, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an den Auftraggeber zu erteilen und der jeweils zuständigen Aufsichtsbehörde eine Vor-Ort-Kontrolle zu ermöglichen. Der Auftraggeber ist über entsprechende geplante Maßnahmen vom Auftragnehmer zu informieren.

(6) Die Parteien sind sich darüber einig, dass die Kontrollmaßnahmen bei einer Verarbeitung von personenbezogenen Daten an mobilen Arbeitsplätzen zur Wahrung der Persönlichkeitsrechte von weiteren Personen an diesen mobilen Arbeitsplätzen primär durch eine Kontrolle der Sicherstellung der vom Auftragnehmer nach Ziff. 8 Abs. 2 und 3 zu treffenden Maßnahmen erfolgt. Anlassbezogen ist dem Auftraggeber auch eine Kontrolle des mobilen Arbeitsplatzes von Beschäftigten durch den Auftragnehmer zu ermöglichen.

10 Unterauftragsverhältnisse

(1) Der Auftragnehmer ist berechtigt, die in der **Anlage 2** zu diesem Vertrag angegebenen Unterauftragnehmer für die Verarbeitung von Daten im Auftrag einzusetzen. Der Wechsel von Unterauftragnehmern oder die Beauftragung weiterer Unterauftragnehmer ist unter den in Absatz 2 genannten Voraussetzungen zulässig.

(2) Der Auftragnehmer hat den Unterauftragnehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten kann. Der Auftragnehmer hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Unterauftragnehmer die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Der Auftragnehmer wird den Auftraggeber im Falle eines geplanten Wechsels eines Unterauftragnehmers oder bei geplanter Beauftragung eines neuen

Unterauftragnehmers rechtzeitig, spätestens aber 4 Wochen vor dem Wechsel bzw. der Neubeauftragung in Textform informieren („Information“). Der Auftraggeber hat das Recht, dem Wechsel oder der Neubeauftragung des Unterauftragnehmers unter Angabe einer Begründung in Textform binnen drei Wochen nach Zugang der „Information“ zu widersprechen. Der Widerspruch kann vom Auftraggeber jederzeit in Textform zurückgenommen werden. Im Falle eines Widerspruchs kann der Auftragnehmer das Vertragsverhältnis mit dem Auftraggeber mit einer Frist von mindestens 14 Tagen zum Ende eines Kalendermonats kündigen. Der Auftragnehmer wird bei der Kündigungsfrist die Interessen des Auftraggebers angemessen berücksichtigen. Wenn kein Widerspruch des Auftraggebers binnen drei Wochen nach Zugang der „Information“ erfolgt, gilt dies als Zustimmung des Auftraggebers zum Wechsel bzw. zur Neubeauftragung des betreffenden Unterauftragnehmers.

(3) Der Auftragnehmer ist verpflichtet, sich vom Unterauftragnehmer bestätigen zu lassen, dass dieser einen Datenschutzbeauftragten gemäß Art. 37 DSGVO benannt hat, sofern der Unterauftragnehmer zur Benennung eines Datenschutzbeauftragten gesetzlich verpflichtet ist.

(4) Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber dem Unterauftragnehmer gelten.

(5) Der Auftragnehmer hat mit dem Unterauftragnehmer einen Auftragsverarbeitungsvertrag zu schließen, der den Voraussetzungen des Art. 28 DSGVO entspricht. Darüber hinaus hat der Auftragnehmer dem Unterauftragnehmer dieselben Pflichten zum Schutz personenbezogener Daten aufzuerlegen, die zwischen Auftraggeber und Auftragnehmer festgelegt sind. Dem Auftraggeber ist der Auftragsverarbeitungsvertrag auf Anfrage in Kopie zu übermitteln.

(6) Der Auftragnehmer ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse (Ziff. 9 dieses Vertrages) des Auftraggebers und von Aufsichtsbehörden auch gegenüber dem Unterauftragnehmer gelten und entsprechende Kontrollrechte von Auftraggeber und Aufsichtsbehörden vereinbart werden. Es ist zudem vertraglich zu regeln, dass der Unterauftragnehmer diese Kontrollmaßnahmen und etwaige Vor-Ort-Kontrollen zu dulden hat.

(7) Nicht als Unterauftragsverhältnisse i.S.d. Absätze 1 bis 6 sind Dienstleistungen anzusehen, die der Auftragnehmer bei Dritten als reine Nebenleistung in Anspruch nimmt, um die geschäftliche Tätigkeit auszuüben. Dazu gehören beispielsweise Reinigungsleistungen, reine Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt, Post- und Kurierdienste, Transportleistungen, Bewachungsdienste. Der Auftragnehmer ist gleichwohl verpflichtet, auch bei Nebenleistungen, die von Dritten erbracht werden, Sorge dafür zu tragen, dass angemessene Vorkehrungen und technische und organisatorische Maßnahmen getroffen wurden, um den Schutz personenbezogener Daten zu gewährleisten. Die Wartung und Pflege von IT-System oder Applikationen stellt ein zustimmungspflichtiges Unterauftragsverhältnis und Auftragsverarbeitung i.S.d. Art. 28 DSGVO dar, wenn die Wartung und Prüfung solche IT-Systeme betrifft, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden und bei der Wartung auf personenbezogenen Daten zugegriffen werden kann, die im Auftrag des Auftraggebers verarbeitet werden.

11 Vertraulichkeitsverpflichtung

(1) Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung der Vertraulichkeit über Daten, die er im Zusammenhang mit dem Auftrag erhält bzw. zur Kenntnis erlangt, verpflichtet.

(2) Der Auftragnehmer hat seine Beschäftigten mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut gemacht und zur Vertraulichkeit verpflichtet.

(3) Die Verpflichtung der Beschäftigten nach Absatz 2 sind dem Auftraggeber auf Anfrage nachzuweisen.

12 Wahrung von Betroffenenrechten

(1) Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich. Der Auftragnehmer ist verpflichtet, den Auftraggeber bei seiner Pflicht, Anträge von Betroffenen nach Art. 12-23 DSGVO zu bearbeiten, zu unterstützten. Der Auftragnehmer hat dabei insbesondere Sorge dafür zu tragen, dass die insoweit erforderlichen Informationen unverzüglich an den Auftraggeber erteilt werden, damit dieser insbesondere seinen Pflichten aus Art. 12 Abs. 3 DSGVO nachkommen kann.

(2) Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten – insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung – durch den Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen. Der Auftragnehmer wird den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nachzukommen.

(3) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch Mitwirkungsleistungen im Zusammenhang mit Geltendmachung von Betroffenenrechten gegenüber dem Auftraggeber beim Auftragnehmer entstehen, bleiben unberührt.

13 Geheimhaltungspflichten

(1) Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.

(2) Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

14 Vergütung

Etwaige Regelungen zu einer Vergütung von Leistungen sind zwischen den Parteien gesondert zu vereinbaren.

15 Technische und organisatorische Maßnahmen zur Datensicherheit

(1) Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind. Dies beinhaltet insbesondere die Vorgaben aus Art. 32 DSGVO.

(2) Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist als **Anlage 3** zu diesem Vertrag beigefügt. Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, wird der Auftragnehmer im Voraus mit dem Auftraggeber abstimmen. Maßnahmen, die lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können vom Auftragnehmer ohne Abstimmung mit dem Auftraggeber umgesetzt werden. Der Auftraggeber kann einmal jährlich oder bei begründeten Anlässen eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

16 Dauer des Auftrags

(1) Der Vertrag beginnt mit Unterzeichnung und läuft für die Dauer des zwischen den Parteien bestehenden Hauptvertrages über die Nutzung der Dienstleistungen des Auftragnehmers durch den Auftraggeber.

(2) Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die anzuwendenden Datenschutzvorschriften oder gegen Pflichten aus diesem Vertrag vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer den Zutritt des Auftraggebers oder der zuständigen Aufsichtsbehörde vertragswidrig verweigert.

17 Beendigung

(1) Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers an diesen zurückzugeben oder zu löschen. Die Löschung ist in geeigneter Weise zu dokumentieren.

(2) Der Auftragnehmer darf personenbezogene Daten, die im Zusammenhang mit dem Auftrag verarbeitet worden sind, über die Beendigung des Vertrages hinaus speichern, wenn und soweit den Auftragnehmer eine gesetzliche Pflicht zur Aufbewahrung trifft. In diesen Fällen dürfen die Daten nur für Zwecke der Umsetzung der jeweiligen gesetzlichen Aufbewahrungspflichten verarbeitet werden. Nach Ablauf der Aufbewahrungspflicht sind die Daten unverzüglich zu löschen.

18 Zurückbehaltungsrecht

Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i.S.d. § 273 BGB hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen wird.

19 Schlussbestimmungen

(1) Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren. Der Auftragnehmer wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.

(2) Für Nebenabreden ist die Schriftform erforderlich.

(3) Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

_____, den	_____	_____, den	_____
Ort	Datum	Ort	Datum

_____	_____
- Auftraggeber -	- Auftragnehmer -

Anlage 1 - Gegenstand des Auftrags

1 Gegenstand und Zweck der Verarbeitung

Der Service „brytes empathy engine“ ermittelt Personalisierungsvorschläge für die Webseite des Auftraggebers auf Basis von Interaktionen des Nutzers mit der Auftraggeber-Webseite. Benutzerstammdaten werden weder erhoben noch verwendet.

Systembedingt wird ein Teil der Kundensystemdaten (u.a. Teile der IP, Browserstack, Endgeräte-Typ, SessionID) für die Ermittlung der Personalisierung genutzt. Personendaten wie Namen, Adressen, Kreditkarten oder ähnliches werden dabei weder ermittelt noch gespeichert oder verwendet.

Der Auftrag des Auftraggebers an den Auftragnehmer umfasst folgende Leistungen:

Auswertung des Verhaltens und der Aktionen von Besuchern der Webpräsenz des Auftraggebers, in die brytes empathy engine-Elemente integriert sind;

regelbasierte Ausspielung sogenannter Nudges (informierende bzw. werbliche HTML-Elemente) auf Grundlage der Verhaltensauswertung und des umgebenden Kontexts;

Pseudonymisierung der Verhaltensdaten und Aggregation zu Reporting- und Optimierungszwecken und zur nutzungsbasierten Abrechnung;

2 Art(en) der personenbezogenen Daten

Folgende Datenarten sind regelmäßig Gegenstand der Verarbeitung:

- Pseudonyme ID
- Warenkorb-Inhalt
- Suchverlauf und -kriterien
- Angesehene Produkte und Seiten
- Bestellte Produkte
- Gezeigte Nudges
- Browsingverhaltens- und Seitennutzungsdaten
- Backend-Anmeldeinformationen der vom Auftraggeber beauftragten Mitarbeiter

3 Kategorien betroffener Personen

Kreis der von der Datenverarbeitung betroffenen Personen:

- Nutzer der E-Commerce- bzw. Online-Präsenz des Auftraggebers, in die die brytes empathy engine integriert ist
- Beauftragte des Auftraggebers mit Zugriff auf das Reporting-Backend

4 Weisungsberechtigte Personen des Auftraggebers

- Beauftragte des Auftraggebers mit Backend-Zugriff

Anlage 2 - Unterauftragnehmer

Der *Auftragnehmer* nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten („Unterauftragnehmer“).

Dabei handelt es sich um nachfolgende(s) Unternehmen:

AMAZON WEB SERVICES EMEA SARL

Marcel-Breuer-Str. 12
80807 München

Tel: +49 89358030
Fax: +49 8935803400

Geschäftsführer: Andrew Isherwood

GmbH-Sitz: München
HRB 242240

Leistung: Infrastrukturbereitstellung

TIMETOACT Software & Consulting GmbH

Im Mediapark 5
50670 Köln

Tel: +49 221 97343 0
Fax: +49 221 97343 20

Geschäftsführer: Felix Binsack, Hermann Ballé

GmbH Sitz: Köln
HRB: 30971

DUNS-ID: 498990092
USt-IdNr.: DE196862443

Leistung: Infrastrukturbetrieb

Anlage 3
Technische und organisatorische Maßnahmen des Auftragnehmers

Der Auftragnehmer trifft nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSGVO.

1 Vertraulichkeit

a. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

i. Standort Köln:

Die Büroräume der synaigy GmbH Standort Köln befinden sich in einem Bürokomplex in Köln. Der Eingang des Gebäudekomplexes ist über Zutrittstüren gesichert, die – bis auf den öffentlichen Eingang – stets verschlossen und selbstschließend sind. Der öffentliche Eingang ist durch einen zentralen Empfang geschützt, der in den Öffnungszeiten dauerhaft besetzt ist. Die Schlösser sind elektronisch und beruhen auf Chipkartentranspondern. Das Chipkartenmanagement für die Zutrittstüren zum Gebäudekomplex liegt beim Vermieter, der Timetoact GmbH. Die vom Vermieter ausgegebenen Chipkarten sind dem jeweiligen Mieter zugeordnet.

Für die Türen zu und in den Geschäftsräumen der synaigy GmbH Standort Köln ist ein eigenes elektronisches Schließsystem im Einsatz.

Diesbezüglich gibt es einen Prozess für die Ausgabe von Chipkarten auf Basis eines 4-Augen-Prinzips. Die Ausgabe von Chipkarten wird protokolliert. Mitarbeiter sind verpflichtet, einen Verlust unverzüglich zu melden. Im Falle eines Verlusts erfolgt eine sofortige elektronische Sperrung des jeweiligen Transponders.

Ferner gibt es einen Prozess bei einem Ausscheiden eines Mitarbeiters, der insbesondere auch die Rückgabe von Transpondern und sonstigem Eigentum der synaigy GmbH durch den ausscheidenden Mitarbeiter beinhaltet.

Außerhalb der Öffnungszeiten sind die Zugänge zum Gebäude (inklusive des Hauptzugangs) nur noch mit Transpondern zu öffnen. Bis auf einen ebenerdigen Zugang und die chipgesicherten Zugänge über die Tiefgaragenstellplätze sind zudem alle Bereiche mit schweren Metallgittern bzw. Glasscheiben abgeriegelt. Die Büroräume der synaigy GmbH befinden sich im 3. Stockwerk des Bürogebäudes.

Die Zutrittsberechtigung wird von einer berechtigten Person genehmigt und innerhalb von 24 Stunden entzogen, nachdem ein Mitarbeiterdatensatz deaktiviert wurde.

Alle Besucher müssen sich ausweisen und registrieren und werden stets von berechtigten Mitarbeitern begleitet. Zutritt zum Gebäude und zu den Räumlichkeiten der synaigy GmbH wird durch Videoüberwachung überwacht.

Daten der synaigy GmbH Standort Köln, die im Auftrag verarbeitet werden, werden entweder auf eigenen Servern vor Ort, in einem Rechenzentrum eines in diesem Vertrag spezifisch als Subunternehmer bezeichneten Dienstleisters oder im Rechenzentrum von Profihost in Deutschland gespeichert. Profihost wird als akkreditierter Telekommunikationsanbieter durch die Bundesnetzagentur als Aufsichtsbehörde überwacht.

Der Zutritt zum gebäudeinternen Serverraum ist durch ein separates mechanisches Schloss gesichert.

ii. Standort Dortmund:

Die Büroräume der synaigy GmbH Standort Dortmund befinden sich in einem alleinstehenden Gebäude in Dortmund. Der Eingang des Gebäudes ist über Zutrittstüren gesichert, die stets verschlossen und selbstschließend sind.

Für die Türen zu und in den Geschäftsräumen der synaigy GmbH Standort Dortmund ist ein eigenes Schließsystem im Einsatz.

Diesbezüglich gibt es einen Prozess für die Ausgabe von Schlüsseln auf Basis eines 4-Augen-Prinzips. Die Ausgabe von Schlüsseln wird protokolliert. Mitarbeiter sind verpflichtet, einen Verlust unverzüglich zu melden. Im Falle eines Verlusts erfolgt ein Austausch der jeweiligen Schließzylinder.

Ferner gibt es einen Prozess bei einem Ausscheiden eines Mitarbeiters, der insbesondere auch die Rückgabe von Schlüsseln und sonstigem Eigentum der synaigy GmbH durch den ausscheidenden Mitarbeiter beinhaltet.

Außerhalb der Öffnungszeiten sind die Zugänge zum Gebäude (inklusive des Hauptzugangs) nur noch mit Schlüsseln zu öffnen. Es sind zudem alle Bereiche (Türen und Fenster) mit Einbruchsalarmeinrichtungen, die zusätzlich einen Sicherheitsdienst benachrichtigen, gesichert. Die Alarmanlage kann nur mit speziellen Token deaktiviert werden, die ebenfalls nach den Regeln für Schlüssel ausgegeben und wieder eingezogen werden. Die Büroräume der synaigy GmbH befinden sich im Gebäude in separaten Bereichen, die für Besucher nur in Begleitung zugänglich sind.

Die Zutrittsberechtigung wird von einer berechtigten Person genehmigt und innerhalb von 24 Stunden entzogen, nachdem ein Mitarbeiterdatensatz deaktiviert wurde.

Alle Besucher müssen sich ggf. ausweisen und werden stets von berechtigten Mitarbeitern begleitet.

Daten der synaigy GmbH Standort Dortmund, die im Auftrag verarbeitet werden, werden entweder auf Servern des synaigy GmbH Standorts Köln, in einem Rechenzentrum eines in diesem Vertrag spezifisch als Subunternehmer bezeichneten Dienstleisters oder im Rechenzentrum von Profihost in Deutschland gespeichert. Profihost wird als akkreditierter Telekommunikationsanbieter durch die Bundesnetzagentur als Aufsichtsbehörde überwacht.

b. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Die Büroräume der synaigy GmbH am Standort Köln befinden sich im dritten Stock. Die Fenster sind nicht durch gegenüberliegende Büros auf gleicher Höhe einsehbar. Die Bildschirme der Mitarbeiter sind stets so ausgerichtet, dass eine Einsichtnahme von außen nicht erfolgen kann.

Die Büroräume der synaigy GmbH am Standort Dortmund befinden sich im Erdgeschoss und ersten Stock. Die Fenster sind nicht durch gegenüberliegende Büros auf gleicher Höhe einsehbar. Die Bildschirme der Mitarbeiter sind stets so ausgerichtet, dass eine Einsichtnahme von außen nicht erfolgen kann.

An jedem IT-System, das bei der synaigy GmbH im Einsatz ist, muss eine vorherige Authentifizierung erfolgen. Dies erfolgt auf Basis eines Benutzernamens und eines Passworts.

Eine Berechtigung zur Nutzung eines IT-Systems oder einer Applikation wird bei der synaigy GmbH nach dem 4-Augen-Prinzip erteilt. Eine Berechtigung muss daher zwingend vom jeweiligen Vorgesetzten für einen Mitarbeiter bei der IT-Administration beantragt werden. Der Vorgesetzte ist verpflichtet, hierbei nur die Berechtigungen zu beantragen, die für den jeweiligen Mitarbeiter unbedingt erforderlich sind, damit dieser die ihm zugewiesenen Aufgaben erfüllen kann. Berechtigungen sind dabei auf das Minimale zu beschränken.

Erteilte Berechtigungen (und der Entzug) werden systemseitig protokolliert. Die Vorgesetzten prüfen regelmäßig, ob die erteilten Berechtigungen noch erforderlich sind. Vorgesetzte sind darüber hinaus verpflichtet, im Falle von Aufgabenwechsel von Mitarbeitern eine entsprechende Korrektur von Berechtigungen bei der IT-Administration zu beantragen.

Im Falle des Ausscheidens von Mitarbeiter informieren die Personalverantwortlichen die IT-Administration unverzüglich über anstehende Veränderungen, damit die IT-Administration entsprechende Berechtigungen entziehen kann. Der Entzug von Berechtigungen muss binnen 24 Stunden nach Ausscheiden eines Mitarbeiters durchgeführt worden sein.

Werden Initialpasswörter vergeben, ist bei der synaigy GmbH stets vorgesehen, dass das Initialpasswort bei der ersten Anmeldung geändert wird. Dies wird technisch erzwungen.

Bei der synaigy GmbH gibt es Richtlinien zur Passwortverwendung, die ebenfalls grundsätzlich technisch erzwungen werden. Passwörter sind komplex zu wählen. Dies beinhaltet die Verwendung von Groß- und Kleinbuchstaben, Sonderzeichen und Ziffern, wobei mindestens 3 von 4 dieser Merkmale erfüllt sein müssen.

Es wird ein Passwortserver betrieben, dessen auch interne Nutzung wird empfohlen. Sollte sich der Stand der Technik bei der Verwendung von Passwörtern ändern, wird die synaigy GmbH die Passwortrichtlinien entsprechend anpassen.

Ein Zugriff auf die externen IT-Systeme findet ausschließlich über verschlüsselte Verbindungen statt. Die dabei verwendeten Verschlüsselungsalgorithmen und Schlüssellängen entsprechen dem Stand der Technik. Für den Fall einer zertifikatsbasierten Zugriffstechnologie ist gewährleistet, dass die Zertifikate durch Mitarbeiter der IT-Administration verwaltet werden.

Alle IT-Systeme, mit denen Daten im Auftrag verarbeitet werden, sind mit Antivirus-Software ausgestattet. Alle Netzwerke sind mit Firewalls geschützt.

c. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Für die Erteilung von Benutzerrechten gilt bei der synaigy GmbH ein Berechtigungskonzept. Dies sieht vor, dass Berechtigungen ausschließlich auf Basis des 4-Augenprinzips und nach dem Minimalprinzip vergeben werden. Dies beinhaltet, dass jeder Mitarbeiter nur die Berechtigungen erhält, die er unmittelbar benötigt, um seine Aufgaben im Unternehmen erfüllen zu können.

Das Berechtigungskonzept ist rollenbasiert. Jedem Mitarbeiter wird grundsätzlich eine bestimmte Rolle zugewiesen. Von dieser Rolle abweichende Berechtigungen müssen begründet sein.

Die Vergabe und der Entzug von Berechtigungen wird protokolliert. Eine quartalsweise Überprüfung erfolgt durch die IT-Administration in Zusammenarbeit mit den jeweiligen Vorgesetzten der Mitarbeitet.

d. Trennung

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Die IT-Systeme, auf denen Daten im Auftrag verarbeitet werden, sind mandantenfähig. Es ist sichergestellt, dass Daten getrennt voneinander verarbeitet werden.

e. Pseudonymisierung & Verschlüsselung

Maßnahmen, die gewährleisten, dass Daten wenn möglich pseudonymisiert und verschlüsselt verarbeitet werden können.

Wo möglich verarbeitet die synaigy GmbH pseudonymisierte Daten statt der Originaldaten. Daten für die Entwicklung und – wo möglich – für Serviceerbringung werden je nach Anwendungsfall anonymisiert, pseudonymisiert oder randomisiert bzw. schon entsprechend vom Auftraggeber angefordert, um für andere als die im Rahmen der Diensterbringung definierten Zwecke für Mitarbeiter der synaigy GmbH oder Dritte unbrauchbar zu sein.

2 Integrität

a. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Jede Eingabe von Daten, die im Auftrag des Auftraggebers von der synaigy GmbH verarbeitet werden, wird wo immer möglich systemseitig unter Zuordnung der jeweiligen Benutzerkennung protokolliert. Gleiches gilt für die Änderung und Löschung von Daten. Im Falle einer Änderung von Daten ist aus der Protokollierung erkenntlich, welche Änderungen vorgenommen wurden.

Die Protokolle werden für die Dauer der Vertragslaufzeit von der synaigy GmbH gespeichert. Eine vorherige Löschung kann zwischen den Parteien vereinbart werden.

Durch die Protokollierung ist jederzeit nachvollziehbar, welche Benutzer Daten eingegeben, geändert oder gelöscht hat.

b. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Dadurch, dass Berechtigungen nach dem Minimalprinzip vergeben werden, ist gewährleistet, dass der Kreis der Personen, die Zugang zu Daten haben, die im Auftrag verarbeitet werden, beschränkt ist.

Jeder Zugriff auf und der Abruf von Daten der Applikation erfolgt verschlüsselt (TLS).

Sofern Daten im Einzelfall auf Anfrage des Auftraggebers an diesen durch die synaigy GmbH übergeben werden soll, werden die Parteien im Vorwege eine Verschlüsselungsmethode bzw. einen Weg der sicheren Übertragung vereinbaren.

3 Verfügbarkeit und Belastbarkeit

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Alle Daten, die für den Auftraggeber verarbeitet werden, befinden sich entweder auf seinen eigenen IT-Systemen oder werden auf von der IT-Abteilung verwalteten Systemen gespeichert. Die synaigy GmbH hat Maßnahmen getroffen, die eine Sicherung der Daten und Wiederherstellung von Daten gewährleistet. Die Datenhaltung erfolgt zudem redundant. Es gibt ein Datensicherungs- und Wiederherstellungskonzept, dessen Wirksamkeit regelmäßig getestet wird.

Im Serverraum sind umfangreiche Maßnahmen zur Gewährleistung der Verfügbarkeit getroffen:

Standort Köln

Es ist eine automatische Branderkennung und -bekämpfung installiert. Das Branderkennungssystem setzt Rauchsensoren in der gesamten Umgebung ein. Alle Stromversorgungssysteme sind redundant. Eine unterbrechungsfreie Stromversorgung (USV) sorgt im Fall eines Stromausfalls dafür, dass kritische Bereiche der Anlage weiterhin mit Strom versorgt werden. Der Serverraum verfügt über Klimatisierung und Temperaturkontrolle.

Es werden vorbeugende Wartungsmaßnahmen durchgeführt, um den fortlaufenden Betrieb der Anlagen zu gewährleisten.

Standort Dortmund:

Da alle Daten nicht vor Ort gehostet werden, sind keine weitergehenden Maßnahmen erforderlich, um einen sofortigen Wiederanlauf zu gewährleisten.

4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Der Schutz personenbezogener Daten und auch der Schutz von Betriebs- und Geschäftsgeheimnissen hat bei der synaigy GmbH eine hohe Priorität. Die Unternehmensleitung hat die Verantwortung für Datenschutz und Informationssicherheit übernommen und eine entsprechende „Leitlinie“ für alle Mitarbeiter herausgegeben.

Ein Prozess zur Durchführung von Datenschutz-Folgenabschätzungen (DSFA) ist definiert und eingerichtet, gleiches gilt für Prozesse hinsichtlich der Beantwortung von Anfragen Betroffener und Umgangs mit Datenschutzverletzungen.

Die Verzeichnisse von Verarbeitungstätigkeiten i.S.d. Art. 30 Abs. 1 und 2 DSGVO werden kontinuierlich aktualisiert.

Alle Mitarbeiter sind auf das Datengeheimnis verpflichtet und an verbindliche Richtlinien zum Umgang mit personenbezogenen Daten gebunden.

Es gibt einen betrieblichen Datenschutzbeauftragten. Alle Mitarbeiter erhalten mindestens eine jährliche Datenschutzschulung bzw. eine „Auffrischung“.

Mitarbeiter, die an der Erbringung von Leistungen für den Auftraggeber beteiligt sind, sind im Hinblick auf die Verarbeitung der Daten instruiert. Sofern der Auftraggeber ergänzende Weisungen erteilt, wird die synaigy GmbH alle betroffenen Mitarbeiter unverzüglich über die jeweilige Weisung informieren und Handlungsanweisungen zur Umsetzung geben.

Die Datenschutzvorkehrungen der synaigy GmbH beinhalten auch eine regelmäßige Überprüfung und Bewertung der getroffenen technischen und organisatorischen Maßnahmen zur Datensicherheit. Hierzu gehört auch ein Verbesserungs- und Vorschlagswesen, an dem sich Mitarbeiter beteiligen können. Die synaigy GmbH gewährleistet so eine kontinuierliche Verbesserung der Prozesse im Umgang mit personenbezogenen Daten.