Vereinbarung über Auftragsverarbeitung i.S.d. Art. 28 Abs. 3 Datenschutz-Grundverordnung (DS-GVO).

STAND 12. NOVEMBER 2022

ZWISCHEN

– IM FOLGENDEN AUFTRAGGEBER –

UND

Kyberio GmbH
Am Mittelfelde 29
30519 Hannover
Deutschland

– IM FOLGENDEN AUFTRAGNEHMER –

Präambel

Diese Vereinbarung konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus dem zwischen den Vertragsparteien bestehenden Verträgen, Vereinbarungen, oder seitens des Auftraggebers erteilten Aufträgen an Kyberio zur Bereitstellung von Dienstleistungen in ihren Einzelheiten beschriebenen Auftragsverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten (»Daten«) des Auftraggebers verarbeiten. Dabei steht die Verarbeitung von personenbezogenen Daten nicht im Fokus der eigentlichen Leistungserbringung der Kyberio GmbH. Durch die erbrachten Dienstleistungen kann jedoch der technische Zugriff auf personenbezogene Daten des Kunden durch Kyberio nicht ausgeschlossen werden. Darüber hinaus können implizit im Rahmen einer Leistungserbringung personenbezogene Daten des Kunden verarbeitet werden (bspw. im Rahmen eines durch Kyberio bereitgestellten Datensicherungsprozesses). Die folgende Vereinbarung regelt den Umgang mit entsprechenden Daten.

§ 1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

Aus dem Vertrag ergeben sich Gegenstand und Dauer des Auftrags sowie Art und Zweck der Verarbeitung. Im Einzelnen können Mitarbeiter der Kyberio GmbH im Rahmen der folgenden Prozesse und Aufgaben mit personenbezogenen Daten des Auftraggebers in Kontakt kommen. Dabei regeln die Leistungsverträge ob und in welchem Umfang die folgenden Aufgaben durch Kyberio wahrgenommen werden:

☐ **Managed Server**

Der Auftragnehmer führt im Auftrag des Auftraggebers Wartungs- und/oder Pflegearbeiten an IT-Systemen des Auftraggebers durch. Der Auftragnehmer greift hierfür via verschlüsselter Netzwerkverbindung auf die für den Auftraggeber betriebenen IT-Systeme zu und

führt Wartungs- und/oder Pflegearbeiten durch. Dabei kann der Zugriff auf im System befindliche personenbezogene Daten nicht ausgeschlossen werden.

Managed Backup

Der Auftragnehmer setzt im Auftrag des Auftraggebers einen Datensicherungsprozess um. Hierfür führt der Auftragnehmer gemäß der Kundenvorgabe (die Frequenz, Umfang und Aufbewahrungszeit betreffend) eine regelmäßige Datensicherung durch, welche personenbezogene Daten enthalten kann. Auf Anfrage des Auftraggebers führt der Auftragnehmer eine Wiederherstellung von gespeicherten Datensicherungen durch. Ebenso führt der Auftragnehmer auf expliziten Auftrag des Auftraggebers gewünschte Löschungen von bestehenden Datensicherungen durch.

Shared Hosting

Der Auftragnehmer stellt dem Auftraggeber eine Webhosting-Umgebung für den Betrieb der Anwendungen des Auftraggebers zur Verfügung. Hierfür führt der Auftragnehmer Wartungs- und/oder Pflegearbeiten der hierfür notwendigen IT-Systeme durch. Dabei kann der Zugriff auf dem System befindlichen personenbezogene Daten nicht ausgeschlossen werden.

Domainverwaltung

Zur Durchführung der im Rahmen der Domainverwaltung notwendigen Tätigkeiten bietet der Auftragnehmer dem Auftraggeber eine Web-Schnittstelle zur Verwaltung der beim Auftragnehmer beauftragten Domains an. In dieser Web-Schnittstelle werden personenbezogene Daten im Rahmen des Verwaltungsprozesses erfasst. Umfang und Art der personenbezogenen Daten werden hierbei von den jeweiligen Registrierungsstellen der beauftragten Top-Level-Domains vorgegeben und vom Auftragnehmer nur zu den notwendigen Zwecken zur Registrierung und dem Betrieb einer Domain verwendet. Hierbei erfolgt in der Regel eine Weitergabe der im System des Auftragnehmers gepflegten personenbezogenen Daten an die jeweilige Registrierungsstelle sowie ggf. dazwischengeschaltete Dienstleister zur Registrierung und Pflege der Domain. Die entsprechende Weitergabe erfolgt nach expliziter Beauftragung durch den Auftraggeber.

Colocation / Remote Hands

Im Rahmen der Colocation- und Remote Hands-Leistungen des Auftraggebers kann der Auftragnehmer temporären Zugriff auf IT-Systeme des Auftraggebers (Remote-Hands) erhalten. Dieser temporäre Zugriff ist beispielsweise zur Fehleranalyse oder -behebung und wird durch den Auftraggeber explizit im Rahmen des Remote-Hand-Prozesses gewährt. Dabei kann der technische Zugriff auf im IT-System eventuell vorhandenen personenbezogenen Daten nicht ausgeschlossen werden. Es ist Aufgabe des Auftraggebers sicherzustellen das die erteilten Berechtigungen nach Beendigung des Remote-Hand-Einsatzes wieder entzogen werden. Darüber hinaus führt der Auftragnehmer, soweit vom Auftraggeber beauftragt, auch Wartungen oder andere manuelle Tätigkeiten an IT-Systemen durch (bspw. Ein- / Ausbau von IT-Systemen, Reparatur von IT-Systemen, Ein- / Ausbau von Komponenten des IT-Systems, insbesondere Austausch oder Ausbau von physischen Datenträgern). Dabei folgt der Auftragnehmer ausdrücklich den Weisungen des Auftraggebers. Das Vorgehen für den Ein-/Ausbau oder Austausch von Datenträgern wird durch den Auftraggeber vorgegeben.

Bereitstellung Virtueller Server

Der Auftragnehmer stellt dem Auftraggeber eine Plattform zum Betrieb virtueller Server (IaaS-Leistung) zur Verfügung. Hierbei kann ein Zugriff auf personenbezogene Daten der Virtualisierungs- und Storage-Ebene technisch nicht ausgeschlossen werden. Der Auftragnehmer darf im Rahmen dieser Bereitstellung jedoch nur die Container verarbeiten (bspw. Migration einer virtuellen Festplatte auf ein anderes Storage) jedoch nicht Daten innerhalb der Container einsehen oder verändern.

Individueller Verarbeitungsgegenstand (falls zutreffend, bitte eintragen)

In allen Fällen gilt, dass eine bewusste Einsichtnahme, Anfertigung einer Kopie, Veränderung, Löschung oder anderweitige Bearbeitung der personenbezogenen Daten ohne vorherige explizite Weisung oder außerhalb des Rahmens der beschriebenen Leistungen durch den Auftraggeber dem Auftragnehmer untersagt ist.

Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit des letzten mit dem Kunden existierenden Vertragsverhältnisses, sofern sich aus den Bestimmungen dieser Anlage nicht darüber hinaus gehende Verpflichtungen ergeben. Sollte der Auftragnehmer eine über den Zeitraum des letzten Vertragsverhältnisses hinausgehend personenbezogene Daten des Auftraggebers verarbeiten so gelten die Regelungen dieser Auftragsdatenvereinbarung bis zur Beendigung der Verarbeitung von personenbezogenen Daten des Auftraggebers durch den Auftragnehmer weiter.

Im Rahmen der obig aufgeführten Leistungen ist nicht ausgeschlossen das der Auftragnehmer Zugriff auf folgende Daten / Datenarten hat:

- ☐ Personenstammdaten
- ☐ Kommunikationsdaten (z.B. Telefon, E-Mail, IP-Adressen)
- ☐ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ☐ Kundenhistorie
- ☐ Vertragsabrechnungs- und Zahlungsdaten
- ☐ Planungs- und Steuerungsdaten (z. B. Bearbeitungsstatus, zu erledigende Aufgaben)
- ☐ Protokolldaten (bspw. IP-Adressen oder Benutzernamen in Serverprotokollen)
- ☐ Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
- ☐ Weitere (vom Kunden ggf. auszufüllen):

Kreis der von der Datenverarbeitung Betroffenen:

- ☐ Kunden
- ☐ Interessenten
- ☐ Abonnenten
- ☐ Beschäftigte / Mitarbeiter
- ☐ Lieferanten / Partner
- ☐ Handelsvertreter
- ☐ Ansprechpartner
- ☐ Weitere (vom Kunden ggf. auszufüllen):

§ 2 Anwendungsbereich und Verantwortlichkeit

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Vertrag und in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwortlicher« im Sinne des Art. 4 Nr. 7 DS-GVO).

(2) Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen. Vom Auftraggeber eingehende Weisungen werden im Ticketsystem des Auftragnehmers durch Eingang einer entsprechenden E-Mail oder eines entsprechenden Dokumentes vom Auftraggeber dokumentiert.

(3) Ein Datenexport darf durch den Auftragnehmer nur gemäß Weisung des Auftraggebers erfolgen. Hierbei hält sich der Auftragnehmer an die Bestimmungen aus Kapitel V (Art. 44-50) der DS-GVO.

§ 3 Pflichten des Auftragnehmers

(1) Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten, außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DS-GVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz-Grundverordnung (Art. 32 DSGVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

(3) Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(4) Der Auftragnehmer unterstützt soweit notwendig, den Auftraggeber im Rahmen seiner Möglichkeiten mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DSGVO sowie bei der Einhaltung der in Art. 33 bis 36 DS-GVO genannten Pflichten. Im Leistungsvertrag können die Parteien hierzu eine Vergütungsregelung treffen. Wird im Leistungsvertrag keine explizite Vergütungsregelung festgehalten erfolgt die Unterstützung durch den Auftragnehmer ohne Vergütung. Unabhängig im Leistungsvertrag festgehaltener Vergütungsregelung erfolgt eine Unterstützung durch den Auftragnehmer immer ohne Vergütung, wenn die Unterstützung aufgrund eines Gesetzes- oder Vertragsverstoßes durch den Auftragnehmer erforderlich wurde.

(5) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und andere für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

(6) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden.

(7) Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

(8) Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

(9) Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DS-GVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

(10) Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese

Datenträger an den Auftraggeber zurück, sofern nicht im Vertrag bereits vereinbart. In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe, Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren, sofern nicht im Vertrag bereits vereinbart.

(11) Daten, exklusiv genutzte Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende zu löschen. Auf Verlangen des Auftraggebers sind diese Daten vorher an den Auftraggeber herauszugeben.

(12) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

(13) Ein Datenexport personenbezogener Daten des Auftraggebers für die Bearbeitung in Drittländern findet durch den Auftragnehmer in der Regel nicht statt. Sollte dies in Ausnahmefällen, z.B. auf expliziten Wunsch des Auftraggebers für die Erbringung spezifischer Leistungen nötig sein, wird dies ausschließlich im Umfang und gemäß Weisungen des Auftraggebers geschehen. Insbesondere hält dabei der Auftragnehmer die Bestimmungen von Kapitel V (Art. 45-50) ein.

§ 4 Pflichten des Auftraggebers

(1) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(2) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, gilt §3 Abs. 10 entsprechend.

(3) Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

§ 5 Anfragen betroffener Personen

(1) Wendet sich eine betroffene Person mit Forderungen zur Berichtigung Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

§ 6 Nachweismöglichkeiten

(1) Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach.

(2) Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne übermäßige Beeinträchtigung des Betriebsablaufs in der Regel nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem unmittelbaren Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht. Für die Unterstützung bei der Durchführung einer Inspektion darf der Auftragnehmer eine Vergütung verlangen, wenn dies im Vertrag vereinbart ist.

(3) Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 2 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

§ 7 Subunternehmer (weitere Auftragsverarbeiter)

(1) Der Einsatz von Subunternehmern als weiteren Auftragsverarbeiter ist nur zulässig, wenn der Auftraggeber vorher zugestimmt hat.

(2) Ein zustimmungspflichtiges Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer weitere

Auftragnehmer mit der ganzen oder einer Teilleistung der im Vertrag vereinbarten Leistung beauftragt. Der Auftragnehmer wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten.

(3) Eine Weitergabe von Aufträgen im Rahmen der in diesem Vertrag vereinbarten Tätigkeiten an Subunternehmer durch den Auftragnehmer erfolgt nicht insoweit im Rahmen der Leistungsvereinbarung keine anderweitige Vereinbarung getroffen wurde.

(4) Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen. Insbesondere obliegt es dem Auftragnehmer die Einhaltung der vom Subunternehmer bereitgestellten Technischen und Organisatorischen Maßnahmen entweder durch regelmäßige Überprüfungen oder entsprechend prüfbare Garantien der Subunternehmer sicherzustellen.

§ 8 Informationspflichten, Schriftformklausel, Rechtswahl

(1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren 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 unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlicher« im Sinne der Datenschutz-Grundverordnung liegen.

(2) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.

(4) Es gilt deutsches Recht.

§ 9 Haftung und Schadensersatz

Eine zwischen den Parteien im Leistungsvertrag (Hauptvertrag zur Leistungserbringung) vereinbarte Haftungsregelung gilt auch für die Auftragsverarbeitung, außer soweit ausdrücklich etwas anderes vereinbart wurde.

Ort. Datum

Unterschrift, Kunde

Ort. Datum

Unterschrift kyberio

Anlage
Technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO

STAND: 02.05.2018

ORGANISATION:

Kyberio GmbH
Am Mittelfelde 29
D-30519 Hannover
Germany
– nachfolgend KYB genannt –

vertreten durch die Geschäftsführer:
Florian Dierks
Simon Künzel

Präambel

KYB kann im Rahmen der Leistungserbringung von KYB mit personenbezogenen Daten in Kontakt kommen. Dabei steht die Verarbeitung von personenbezogenen Daten nicht im Fokus der eigentlichen Leistungserbringung der KYB. Durch die erbrachten Dienstleistungen kann jedoch der technische Zugriff auf personenbezogene Daten des Kunden durch KYB nicht ausgeschlossen werden. Gemäß Artikel 32 DSGVO hat KYB technische und organisatorische Maßnahmen zu treffen wann immer personenbezogene Daten verarbeitet werden. Diese sind erforderlich um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten.

KYB erfüllt diesen Anspruch durch die im Folgenden dokumentierten Maßnahmen:

1. Vertraulichkeit gem. Art. 32 Abs. 1 lit. b DSGVO

a. Zutrittskontrolle

Der Zugang zum Haupteingang der KYB sowie sämtlicher Nebeneingänge ist durch einen Zaun physikalisch beschränkt. Die Türen und Tore durch den Zaun sind immer verschlossen und können nur mit Transpondern von Mitarbeitern der KYB Vorort geöffnet werden. Darüber hinaus können das Haupttor sowie der Haupteingang des Zauns via Klingel und daran gekoppelte manuelle Öffnungsfunktion durch KYB-Mitarbeiter im Network-Operation-Center (NOC) geöffnet werden.

Sämtliche Zugangswege zu Gebäudeeingängen der KYB sind via Videoüberwachung gesichert. Die Mitarbeiter des NOCs haben 24/7 eine Live-Darstellung aller Kameras auf dafür dedizierten Bildschirmen im NOC.

Die Zugänge zum Gebäude sind stets verschlossen und können von außen nur mit Sicherheitsschlüsseln geöffnet werden. Der Zugang zum Gebäude wird rund um die Uhr durch qualifizierte Mitarbeiter am zentralen Empfang / NOC überwacht und jeder Mitarbeiter, Kunde oder Lieferant muss sich am Empfang anmelden. Bei Anmeldung erhält der Besucher einen Besucherausweis den er bei Verlassen des Gebäudes wieder abzugeben hat. Besucher werden hierbei bereits über die Hausordnung unterrichtet. Besucher müssen entweder angemeldet sein oder über die Berechtigungen zu einer Eigenanmeldung verfügen. Die Authentizität von Besuchern wird mittels gültigem Lichtbildausweis überprüft. Besucher werden von einer Mitarbeiterin oder einem Mitarbeiter persönlich am Empfang abgeholt. Organisatorisch ist geregelt, dass Fremde sich im Gebäude niemals allein aufhalten oder frei bewegen dürfen.

Der Zutritt zu den Rechenzentrumsflächen ist über eine Zutrittskontrollanlage gesichert und nur Mitarbeitern der KYB alleine möglich. Für das Rechenzentrum Am Mittelfelde 29 ist diese Zutrittskontrolle als 2-Faktor-Authentifizierung ausgelegt. Jeder Zutritt wird protokolliert. Zutrittsprotokolle und Videoaufzeichnungen werden einmal täglich für die zurückliegenden 24 Stunden durch Mitarbeiter der KYB kontrolliert.

Außerhalb der Arbeitszeiten erfolgt die Überwachung der Räumlichkeiten durch eine Alarmanlage gemäß VDE-Norm. Meldungen der Anlage werden durch einen Sicherheitsdienst überwacht und nach einem dokumentierten Interventionsplan verfolgt. Bei sämtlichen technischen Räumlichkeiten, den Zugangswegen sowie für den Perimeterschutz besteht eine zusätzliche Videoüberwachung. Diese ist insbesondere in allen Räumlichkeiten des Rechenzentrums vorhanden und wird durch zusätzliche Bewegungssensoren unterstützt.

b. Zugangskontrolle

Unbefugten wird der Zugang zu Datenverarbeitungssystemen nicht gewährt. Der Zugang über Außenschnittstellen zu unseren EDV-Systemen ist durch eine Firewall geschützt. Sensible Dienste die nicht öffentlich erreichbar sein müssen werden durch den Einsatz eines VPN abgesichert. Öffentlich erreichbare Systeme, wie E-Mail oder Internetzugang werden über entsprechende Trennungen von anderen Diensten isoliert. KYB betreibt je nach Sicherheitsklassifikation diverse, teilweise physisch vollständig entkoppelte Netzwerke. Sämtliche Systeme sind passwortgeschützt und verfügen über benutzerspezifische Zugänge. Gruppenzugänge werden nicht genutzt. Neben dem Einsatz starker Passwörter auf Basis interner Passwortvorgaben wird ein 2-Faktor-System zur Authentifizierung an sensiblen Systemen der KYB genutzt. Die Passwort-Richtlinien der KYB definiert neben der geforderten Passwortkomplexität auch Rahmenparameter wie das zwangsweise Neusetzen eines Passwortes in definierten Fristen sowie den Verbot der Wiederverwendung eines Passwortes. Die Detaillierung der Zugriffsberechtigungen zu dem Equipment des Vertragspartners erfolgt gemäß der Weisung des Auftraggebers auf Basis der von KYB zu erbringenden Leistungen. Gemäß der internen Richtlinien der KYB erfolgen je nach Systemart und Einstufung unterschiedliche Reaktionen auf Fehlversuche bei der Anmeldung. Neben der zeitweisen Sperrung, dem dynamischen Hinzufügen von Netzwerk-Sperren, oder der vollständigen Sperrung eines Zugangs erfolgt auch eine Protokollierung und Alarmierung.

c. Zugriffskontrolle

Der Zugriff auf Netzwerkverzeichnisse oder Systeme, in denen personenbezogene Daten gespeichert werden, ist auf die jeweiligen Personen beschränkt, die mit den Aufträgen beschäftigt sind, für die solche Daten verwendet werden sollen. Dabei muss jeder Benutzer sich mit personenspezifischen Zugangsdaten authentifizieren. Die initiale Zugriffsmöglichkeit ist, wo immer dies aufgrund der Funktion des Systems und den Vorgaben des Kunden realisiert werden kann, immer auf das interne Netzwerk der KYB beschränkt. Im Falle einer externen Einwahl (VPN) in die internen Netzwerke der KYB erhält der Mitarbeiter lediglich Zugriff auf für ihn relevante Netzbereiche. Im Falle eines externen Zugriffs erfolgt die Authentifizierung darüber hinaus auf Basis einer 2-Faktor-Authentifzierung. Für den Zugriff auf die Systeme und das Equipment des Kunden werden kundenindividuelle Maßnahmen mit dem jeweiligen Kunden abgestimmt. Die Allgemeinen Zugriffswege für den Zugriff eines KYB-Mitarbeiters auf Systeme oder Instanzen des Kunden – soweit der Beauftragung entsprechend – werden mindestens mittels starker Verschlüsselung abgesichert.

Mitarbeiter der KYB erhalten dabei auf Basis definierter Berechtigungen je Anwendung / System nur die notwendigen Berechtigungen. Es wird klar zwischen Administratoren einer Anwendung / eines Systems und weiteren Benutzergruppen unterschieden. Die Berechtigungen werden halbjährlich im Rahmen des internen Revisionsprozesses sowohl auf Notwendigkeit als auch auf korrekte Konfiguration überprüft.

d. Trennungskontrolle

KYB verarbeitet eigene personenbezogene Daten immer nur innerhalb der für die konkrete Aufgabe notwendigen Systeme und Prozesse. Im Rahmen der eigenen Verarbeitung von personenbezogenen Daten trennt KYB Test-Umgebungen von Produktiv-Umgebungen. Je nach erbrachter Leistung isoliert KYB Kundendaten entweder physisch (separate Hardware-Systeme, bspw. „Hosting dedizierter Server“) oder logisch. Eine logische Isolierung kann hier je nach erbrachter Leistung unterschiedlich realisiert werden („Virtuelle Server“, „Mandantenfähige Software“). Eine darüberhinausgehende Trennungskontrolle für die Speicherung und Verarbeitung von personenbezogenen Daten im Rahmen der Auftragsverarbeitung obliegt dem Auftraggeber.

2. Integrität gem. Art. 32 Abs 1 lit. b DSGVO

a. Weitergabekontrolle

Personenbezogene Daten oder anderweitig vertrauliche Daten werden bei der Übertragung mindestens mittels einer Transportverschlüsselung verschlüsselt. KYB verfügt über eine interne Richtlinie zum Einsatz

von Kryptographie-Verfahren mit klaren Vorgaben welche Kryptographie-Verfahren in welchen Konstellationen mit welchen technischen Details zulässig sind. Dabei orientiert sich KYB an den Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sowie dem National Institute of Standards and Technology (NIST).

Darüber hinaus empfiehlt KYB bei der Übertragung von personenbezogenen Daten im Kundenkontakt zusätzlich eine dateibasierte Verschlüsselung zu verwenden. So wird auch eine temporäre Ablage der Daten auf KYB oder Kundenseite abgesichert. Dies setzt jedoch die technische Fähigkeit des Kunden zur Annahme oder Übermittlung einer entsprechend verschlüsselten Datei voraus. Soweit KYB diese Möglichkeit mit dem Kunden feststellt, wird KYB eine solche mit dem Kunden abgestimmte Methode zur dateibasierten Verschlüsselung verwenden.

KYB verfügt über einen Standard-Prozess zur Verwahrung sowie der Löschung oder physischen Vernichtung von Datenträgern. Hierbei werden sowohl der Datenträger als auch der sichere Verwahrort sowie die anschließende Rückübermittlung, Löschung, oder Vernichtung protokolliert. Die Vernichtung erfolgt gemäß Sicherheitsstufe H-4 DIN 66399-2.

Der Versand personenbezogener Daten erfolgt ausschließlich im gesetzlich vorgesehenen Rahmen. Mobile Datenträger mit personenbezogenen Daten werden nur in gesicherten Räumen gehalten, bei Nichtverwendung im Tresor. Daten, die für eine Auftragsdurchführung nicht mehr benötigt werden, wie z.B. gesperrte Daten, werden in einem separierten zugriffsgeschützten Speicherbereich abgelegt.

Datenträger oder Hardware werden nur durch entsprechend verpflichtete und zertifizierte Unternehmen repariert oder entsorgt. Gleiches gilt für die Entsorgung von Daten auf Papier.

b. Eingabekontrolle

Nur ausgewählte Mitarbeiter können in einem Kundenprojekt auf die Systeme und Daten des Kunden zugreifen. Dabei werden nur Mitarbeiter ausgewählt, die auch für die Erbringung der vertraglich zugesicherten Leistung direkt notwendig sind. Die Legitimation der Mitarbeiter ergibt sich aus der Zuordnung zur Gruppe der für diesen Kunden zuständigen Mitarbeiter. Alle Mitarbeiter sind dabei auf die Vertraulichkeit und Einhaltung der gesetzlichen sowie internen Regelungen verpflichtet.

Arbeiten an den Kundensystemen werden protokolliert. Wo technisch möglich erfolgt eine automatische Protokollierung aller Veränderungen und Aktionen. Darüber hinaus erfolgt eine manuelle Protokollierung der Mitarbeiter. Dies wird regelmäßig Stichprobenhaft überprüft.

Die Standard-Arbeitsanweisung an Mitarbeiter ist keine personenbezogenen Daten der Kunden zu verändern oder zu manipulieren. Dies darf nur auf explizite Weisung des Kunden erfolgen. Davon ausgenommen sind Regelprozesse zur Verwaltung von Daten (Datensicherung, Löschung von Protokolldaten nach vertraglich festgelegter Aufbewahrungszeit etc.), die im Rahmen des Betriebes der Kundeninstanzen in Standard-Logdateien der eingesetzten Serversoftware anfallen und ebenfalls personenbezogene Daten enthalten können.

3. Verfügbarkeit und Belastbarkeit gem. Art. 32 Abs 1 lit. b DSGVO

a. Verfügbarkeitskontrolle

KYB verfügt über zwei physisch voneinander unabhängige und räumlich getrennte Rechenzentren. Die Sicherstellung der Verfügbarkeit kundenspezifischer Daten erfolgt im Rahmen der vertraglich definierten Anforderungen. KYB betreibt hierfür Datensicherungsspeicher in beiden Rechenzentren, um Datensicherungen über Kreuz zu ermöglichen. Datensicherungsintervalle sind dabei individuell vertraglich mit dem Kunden gestaltbar. Für IT-Systeme und Daten der KYB, die zum Betrieb des Rechenzentrums und somit zur Sicherstellung der Verfügbarkeit von Kundensystemen und –daten ebenfalls notwendig sind, erfolgt eine tägliche über Kreuz-Sicherung mit zusätzlicher Sicherung aller geänderten Daten nachdem Arbeiten an den KYB-Systemen durchgeführt wurden. Darüber hinaus werden die Storage-Systeme, auf denen Kundensysteme betrieben werden, standardmäßig mit fehlertoleranten RAID-Systeme vor Datenverlust geschützt. Hier kann es je nach vertraglicher Individualkonfiguration bei Kunden jedoch Abweichungen geben. Für vom Auftraggeber von Dritten gemietete EDV-Systeme oder vom Auftraggeber eingestellte EDV-Systeme ist der Auftraggeber verantwortlich. Um das Ausmaß möglicher Brandschäden zu minimieren, ist unser Unternehmen mit einer Brandmeldeanlage ausgestattet. Meldungen der Anlage werden durch einen Sicherheitsdienst überwacht und nach

einem dokumentierten Interventionsplan verfolgt. Die Klimaanlagen sind N+1 vorhanden und werden durch ein Notstromaggregat versorgt.

Beide Rechenzentrumsstandorte verfügen über USV-Systeme, sowie eine Notstromersatzanlage.

KYB betreibt im Rahmen eines aktiven Information Security Management Systems nach ISO-27001 auf Basis IT-Grundschutz eine aktive Notfallvorsorge. Hierzu gehört neben der kontinuierlichen Weiterent wicklung des Notfallhandbuchs auch die regelmäßige Durchführung von Notfallübungen. Diese erfolgen mindestens zweimal im Jahr und werden als detaillierte Planspiele umgesetzt. Mindestens einmal im Jahr erfolgt darüber hinaus ein sogenannter „Black Building Test" um einen vollständigen Stromausfall zu simulieren. Die Durchführung der Übungen sowie der darin gewonnenen Erkenntnisse werden protokolliert.

KYB überwacht die Verfügbarkeit jeglicher Systeme zum Betrieb der Rechenzentren. Darüber hinaus überwacht KYB im Standard auch die Verfügbarkeit von Kundensystemen. Der Umfang dieses Monitorings wird dabei im Rahmen der Vertragsgestaltung / Angebotsphase durch den Kunden festgelegt und kann auch in einer bestehenden Vertragsbeziehung jederzeit angepasst werden. Neben einer zeitnahen Alarmierung bei Ausfall oder Störung entsprechender Systeme oder Anwendungen kann KYB so auch die Verfügbarkeit eines Systems oder einer Anwendung nachweisen.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

a. Datenschutz-Management

KYB betreibt ein Datenschutz-Management-System. Hierfür stellt KYB einen Datenschutzbeauftragten der das Datenschutz-Management-System betreut und direkt an die Geschäftsleitung berichtet. Im Rahmen des Datenschutz-Management-Systems dokumentiert KYB jegliche Verfahren und Prozesse mit Verarbeitung von personenbezogenen Daten in Unternehmensinternen Verfahrensverzeichnissen. Ebenso betreibt KYB ein ISMS nach ISO-27001 auf Basis IT-Grundschutz und ist nach diesem Standard durch das Bundesamt für Sicherheit in der Informationstechnik zertifiziert worden. Das Zertifikat wird in jährlichen Intervallen überprüft und alle 3 Jahre neu beantragt und geprüft. Technische organisatorische Maßnahmen werden jährlich überprüft, unter anderem auch im Rahmen der Zertifikatsüberprüfung.

Im Rahmen des Datenschutz-Management-Systems nimmt KYB bei identifizierten Bedarf Datenschutz-Folgenabschätzungen vor.

Darüber hinaus hat KYB alle Mitarbeiter zur Einhaltung der Vertraulichkeit und der Datenschutzgesetze schriftlich verpflichtet und erneuert diese Verpflichtung jährlich. Ebenso ist ein regelmäßiger Sensibilisierungsund Schulungsprozess aller Mitarbeiter etabliert.

b. Incident-Response-Management

KYB betreibt im Rahmen des etablierten ISMS einen dokumentierten Prozess zum Incident-Response-Management. Neben Eskalations- und Meldewegen beinhaltet dieser Prozess die Nachbetrachtung und Analyse und anschließende Optimierung auf Basis gewonnener Erkenntnisse.

Zur Erkennung von Incidents setzt KYB sowohl gerätebasierte als auch netzwerkbasierte Lösungen ein (Intrusion-Detection, Virus- und Malware-Erkennung, Anti-Spam-Filter sowie Anomalie-Detektionen). Darüber hinaus überwacht KYB die Infrastruktur und Kundensysteme mit einer Monitoring-Lösung auf Störungen und Anomalien.

Alle Incidents werden im Rahmen des Incident-Response-Management-Systems in einem Ticketsystem dokumentiert. Sowohl der Datenschutzbeauftragte (wenn personenbezogene Daten betroffen sind) als auch der IT-Sicherheitsbeauftragte sind im Rahmen des Eskalationsprozesses einzubinden.

c. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

KYB verfolgt das Prinzip der Datenminimierung. So werden nur Daten die für den jeweiligen Prozess/Kontext notwendig sind verarbeitet und gespeichert. Die Angemessenheit wird regelmäßig durch den Datenschutzbeauftragten geprüft. Alle Berechtigungen werden nach einem „Need-to-have"-Prinzip vergeben und müssen begründet werden. Die Vergabe von Berechtigungen wird regelmäßig im internen Revisionsprozess überprüft und hinterfragt.

Speicher- und Löschfristen werden aktiv definiert. Deren Einhaltung wird durch den Datenschutzbeauftragten geprüft.

d. Auftragskontrolle (Outsourcing an Dritte)
KYB prüft (Unter-)Auftragnehmer im Rahmen des Auswahlprozesses sowie in der kontinuierlichen Zusammenarbeit auf angemessene Datenschutz- und IT-Sicherheitsprozesse. Hierzu nimmt KYB neben einer Sorgfaltsprüfung im Auswahlprozess eines (Unter-)Auftragnehmers auch Stichprobenprüfungen (Dokumentation und Vor-Ort) bei (Unter-)Auftragnehmern vor.

KYB verpflichtet jegliche (Unter-)Auftragnehmer vertraglich sowohl auf die geltenden Vertraulichkeitsverpflichtungen als auch auf die Einhaltung des Datenschutzes. Entsprechend wird für alle (Unter-) Auftragnehmer mit Bezug zu personenbezogenen Daten eine Auftragsvereinbarung geschlossen.

Kyberio GmbH

– Die Geschäftsführung -