Datenschutzbedingungen für Auftragsverarbeitung
der easy Informations- und Bürotechnik GmbH

- nachfolgend als „easy“ bezeichnet –

im Sinne des Art. 28 Abs. 3 Datenschutz-Grundverordnung (DS GVO).

Präambel

Diese Vereinbarung konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der im Hauptvertrag mit den Kunden 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.

1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

1.1 Aus dem Vertrag ergeben sich Gegenstand und Dauer des Auftrags sowie Art und Zweck der Verarbeitung. Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit des Vertrages, sofern sich aus den Bestimmungen dieser Vereinbarung nicht darüber hinausgehende Verpflichtungen ergeben.

2 Anwendungsbereich und Verantwortlichkeit

2.1 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).

2.2 (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.

3 Pflichten des Auftragnehmers

3.1 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 Art. 28 Abs. 3 lit. 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.

3.2 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 DS-GVO) 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. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer

vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

3.3 Der Auftragnehmer unterstützt soweit vereinbart den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der Datenschutz-Grundverordnung sowie bei der Einhaltung der in Artt. 33 36 DS GVO genannten Pflichten.

3.4 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.

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

3.6 Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

3.7 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.

3.8 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.

3.9 Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen. Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.

4 Pflichten des Auftraggebers

4.1 Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. daten- schutzrechtlicher Bestimmungen feststellt.

4.2 Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, gilt §3 Abs. 10 entsprechend. (Anmerkung: Im Vertrag können die Parteien hierzu eine Vergütungsregelung treffen).

4.3 Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

5 Anfragen betroffener Personen

5.1 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 soweit vereinbart. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

6 Nachweismöglichkeiten

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

6.2 Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und 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 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. Der Aufwand einer Inspektion ist für den Auftragnehmer grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.

6.3 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)

7.1 Der Einsatz von Subunternehmern als weiteren Auftragsverarbeitern ist nur zulässig, wenn der Auftraggeber vorher zugestimmt hat.

7.2 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.

7.3 Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung folgender Subunternehmer durchgeführt:

Name und Anschrift des Subunternehmers	**Beschreibung der Teilleistungen**
Canon Deutschland GmbH Europark Fichtenhain A 10 47807 Krefeld	Online-System zur Informations- und Dokumentenverwaltung „Therefore Online“ (Saas – Software as a Service, Cloud Servies), Fleetmanagement, cloud-basierte Druck- und Scanlösungen
Securepoint GmbH Bleckeder Landstraße 28 21337 Lüneburg	Antivirus-Programm, Awareness-Training Cyber Security
Krämer IT Solutions GmbH Koßmannstraße 7 66571 Eppelborn	Monitoring, Patch-Management im Rahmen Managed IT Servies
TERRA CLOUD GmbH Hankamp 2 32609 Hüllhorst	Rechenzentrumsleistungen, Microsoft 365 Produkte
Ibeco-Systems GmbH August-Euler-Str. 7 50259 Pulheim	Rechenzentrumsleistungen, Cloud-Infrastruktur, Hosted Exchange, E-Mail Archivierung, Backup
MLF Mercator-Leasing GmbH & Co. Finanz-KG Londonstraße 1 97424 Schweinfurt	Finanzierung (Miete, Leasing)

Name und Anschrift des Subunternehmers	Beschreibung der Teilleistungen
abcfinance advice GmbH Adolf-Grimme-Allee 3 50829 Köln	Finanzierung (Miete, Leasing)
(1) Deutsche Bank AG Georgsplatz 20 30159 Hannover (2) Hannoversche Volksbank eG Kurt-Schumacher-Straße 19 30159 Hannover	Zahlungsabwicklung
DPD Deutschland GmbH Wailandtstraße 1 63741 Aschaffenburg	Paketversand

Vor der Hinzuziehung weiterer oder der Ersetzung aufgeführter Subunternehmer holt der Auftragnehmer die Zustimmung des Auftraggebers ein, wobei diese nicht ohne wichtigen datenschutzrechtlichen Grund verweigert werden darf.

7.4 Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen.

8 Informationspflichten, Schriftformklausel, Rechtswahl

8.1 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.

8.2 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.

8.3 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.

8.4 Es gilt deutsches Recht.

9 Haftung und Schadenersatz

9.1 Auftraggeber und Auftragnehmer haften gegenüber betroffener Personen entsprechend der in Art. 82 DS GVO getroffenen Regelung.

10 Anlage – Technische und organisatorische Maßnahmen

Nr.	Gebiet	Beschreibung
0	**Organisation**	

Nr.	Gebiet	Beschreibung
	Wie ist die Umsetzung des Datenschutzes organisiert?	Die Geschäftsführung stellt die Ausführung, Umsetzung sowie Kontrollfunktionen aus dem BDSG (neu DSG-VO) sicher.
	Nennen Sie uns bitte den Namen und die Kontaktdaten Ihres Datenschutzbeauftragten.	Jörg Volmer, Emmy-Noether-Straße 8, 31515 Wunstorf, Tel. +49 5031 96234 0
	In welcher Form werden die Mitarbeiter auf die Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen geschult, die für diese Verarbeitung in Anwendung kommen?	Das Schulungskonzept beinhaltet sowohl eine Datenschutzunterweisung bei Beginn der Tätigkeit (20.04.2018), als auch eine konstante Sensibilisierung durch regelmäßige Meetings, fachbezogenen Schulungen und persönliche Sensibilisierung durch die Geschäftsleitung.
	Sind die Verarbeitungen hinsichtlich datenschutzrechtlicher Zulässigkeit dokumentiert?	Im Rahmen der internen Verfahrens- und Arbeitsanweisungen sind die Datenströme dokumentiert und die Zulässigkeit der Verarbeitung und Nutzung nach BDSG nachgewiesen. Ggf. erforderliche Vorabkontrollen werden bereits im Planungsstadium integriert.
1	**Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)**	
1.1	**Zutrittskontrolle**	
	Wie werden die Gebäude, in denen die Verarbeitung stattfindet, vor unbefugtem Zutritt gesichert?	Das Gelände ist vollflächig umzäunt und mit einem Tor gesichert. Das Gebäude ist mit einer elektronischen Schließ- und Zutrittskontroll-anlage sowie Videokameras ausgerüstet
	Wie werden die Räume / Büros, in denen die Verarbeitung stattfindet, vor unbefugtem Zutritt gesichert?	Die betroffenen Räume werden ebenfalls durch ein Sicherheitsschließsystem gesichert. Dokumente werden in abschließbaren Möbeln verwahrt.
	Wie werden die Verarbeitungsanlagen vor unbefugtem Zugriff geschützt?	Es wird primär auf einem Terminalserver gearbeitet (es befinden sich keine sensiblen Daten auf dem lokalen Computer). Weiterhin sind sämtliche Speichermedien passwortgeschützt.
	Wie werden die umgesetzten Zutrittskontrollmaßnahmen auf Tauglichkeit geprüft?	Im Rahmen permanenter Kontrollen durch die Geschäftsleitung werden die Zutrittskontrollsysteme sowie Schließanlagen fortwährend geprüft.
1.2	**Zugangskontrolle**	
	Wie erfolgt die Vergabe von Benutzerzugängen?	Benutzerzugänge werden nur selektiv und durch die Geschäftsleitung in Kooperation mit der IT-Abteilung vergeben. Rechtevergabe und Änderung

Nr.	Gebiet	Beschreibung
		sind dokumentiert. Zugriff auf kaufmännische Dokumente und Kommunikationsformen sind durch Passwörter geschützt.
	Wie wird die Gültigkeit von Benutzerzugängen überprüft?	Eine regelmäßige Revision der vergebenen Rechte ist Teil der Prüfungen der Maßnahmen und wird zusammen mit der GL durchgeführt und von dieser dokumentiert. Passwörter müssen regelmäßig erneuert werden.
	Wie werden Benutzerzugänge inkl. Antragstellung, Genehmigungsverfahren etc. dokumentiert?	Die Anlage und Veränderung von Benutzerzugängen wird in firmeneigenen Formularen dokumentiert und hinterlegt.
	Wie wird sichergestellt, dass die Anzahl von Administrationszugängen ausschließlich auf die notwendige Anzahl reduziert ist und nur fachlich und persönlich geeignetes Personal hierfür eingesetzt wird?	Die Entscheidungen zur Rechtevergabe halten sich streng an die entsprechenden Vorgaben, Datenvermeidung und Datensparsamkeit, weniger ist hier oft mehr.
	Ist ein Zugriff auf die Systeme / Anwendungen von außerhalb des Unternehmens möglich (Heimarbeitsplätze, Dienstleister etc.) und wie ist der Zugang gestaltet?	Ein Zugang zur Fernwartung der Systeme ist über geschützte VPN-Zugänge realisiert.
1.3	**Zugriffskontrolle**	
	Wie wird erreicht, dass Passwörter nur dem jeweiligen Benutzer bekannt sind?	Die Passwörter werden vom jeweiligen Mitarbeiter selbst vergeben. Die strengen Systemvoreinstellungen zwingen zu einer hohen Passwortkomplexität. Passwörter werden nicht gespeichert.
	Welche Anforderungen werden an die Komplexität von Passwörtern gestellt?	Die Vorgaben Empfehlungen des BSI dienen als Vorbild für die o.g. Systemeinstellungen. Passwörter müssen Buchstaben, Ziffern und Sonderzeichen enthalten und in regelmäßigen Abständen geändert werden.
	Wie wird gewährleistet, dass der Benutzer sein Passwort regelmäßig ändern kann / muss?	Systemeinstellungen (Vorgaben).
	Welche organisatorischen Vorkehrungen werden zur Verhinderung von unberechtigten Zugriffen auf personenbezogene Daten am Arbeitsplatz getroffen?	Schulung und Sensibilisierung der Mitarbeiter. Einweisungen und regelmäßige Schulungen zu den verwendeten Geräten. Datenschutzvereinbarungen für alle Mitarbeiter.
	Wie wird sichergestellt, dass Zugriffsberechtigungen anforderungsgerecht und zeitlich beschränkt vergeben werden?	Siehe auch Punkt Vergabe von Benutzerzugängen Punkt 1.2; die GL prüft in regelmäßigen Abständen die Rechte und Benutzerstruktur.

Nr.	Gebiet	Beschreibung
	Wie erfolgt die Dokumentation von Zugriffsberechtigungen?	Reports aus dem Berechtigungssystem (Passwortmanager) durch den Administrator.
	Wie wird sichergestellt, dass Zugriffsberechtigungen nicht missbräuchlich verwendet werden?	Sporadische Durchsicht der Systemprotokolle durch die IT-Abteilung und GL.
	Wie lange werden Protokolle aufbewahrt? Wer hat Zugriff auf die Protokolle und wie oft werden sie ausgewertet?	Keine festgelegten Fristen, meist Systemparameter, ausschließlich die Geschäftsführung
1.4	**Trennungskontrolle**	
	Wie wird sichergestellt, dass Daten, die zu unterschiedlichen Zwecken erhoben wurden, getrennt voneinander verarbeitet werden?	Unterschiedliche, thematisch getrennte Tabellen im System.
1.5	**Pseudonymisierung**	
	Welche organisatorischen Maßnahmen wurden getroffen, damit die Verarbeitung personenbezogener Daten gesetzeskonform erfolgt?	Alle mit der Verarbeitung von personen-bezogenen Daten betrauten Personen wurden entsprechend verpflichtet. Ein Datenschutzkonzept wird im Unternehmen eingesetzt und ist allen Mitarbeitern bekannt gemacht. Das Schulungskonzept beinhaltet sowohl eine Datenschutzunterweisung bei Beginn der Tätigkeit, als auch eine konstante Sensibilisierung durch fachbezogene Meetings und persönliche Sensibilisierung durch die Geschäftsleitung.
	Wie werden personenbezogene Daten verarbeitet /aufbewahrt, sodass diese nicht den betroffenen Personen zugeordnet werden können?	Im System können Daten auf Wunsch verschlüsselt werden. Die Daten sind jedoch nicht von Grund auf pseudonymisiert.
2	**Integrität (Art. 32 Abs. 1 lit. b DS-GVO)**	
2.1	**Weitergabekontrolle**	
	Wie gewährleisten Sie die Integrität und Vertraulichkeit bei der Weitergabe von personenbezogenen Daten?	Es werden Datenschutzvereinbarungen mit externen Partnern getroffen.
	Werden Verschlüsselungssysteme bei der Weitergabe von personenbezogenen Daten eingesetzt und wenn ja, welche?	Wenn ein Zugang zum System gewährt wird, dann mit passwortgesichertem VPN-Zugang.
	Wie wird die Weitergabe personenbezogener Daten dokumentiert?	Über Protokolle und die Datenschutz-vereinbarungen.
	Wie wird der unberechtigte Abfluss von personenbezogenen Daten durch technische Maßnahmen beschränkt?	Eine strikte Rechtevergabe sichert die Daten vor unberechtigtem Zugriff. Weiterer Schutz durch eine Firewall.

Nr.	Gebiet	Beschreibung
	Gibt es ein Kontrollsystem, das einen unberechtigten Abfluss von personenbezogenen Daten aufdecken kann?	Dies wird im Rahmen der Kontrollen unter Punkt 1 mit geprüft.
2.2.	**Eingabekontrolle**	
	Welche Maßnahmen werden ergriffen, um nachvollziehen zu können, wer wann und wie lange auf Applikationen zugegriffen hat?	Wird im System protokolliert.
	Wie ist nachvollziehbar, welche Aktivitäten auf den entsprechenden Applikationen durchgeführt wurden?	Rollen-/Rechtekonzepte und diverse Lizenz-Modelle mit unterschiedlichen Berechtigungs-Konzepten und Sicherung der Aktivitäten auf Datenbankebene.
	Welche Maßnahmen werden ergriffen, damit die Verarbeitung durch die Mitarbeiter nur gemäß der Weisungen des Auftraggebers erfolgen kann?	Zugriffskontrolle anhand des Rollen-/Rechte-Konzepts zur ordnungsgemäßen Datenbear-beitung und Speicherung
	Welche Maßnahmen werden getroffen, damit auch Unterauftragnehmer ausschließlich im vereinbarten Umfang personenbezogene Daten des Auftraggebers durchführt?	Sämtliche Unterauftragnehmer unterliegen den gleichen Vorgaben wie der Auftragnehmer. Entsprechende Verträge und Datenschutz-vereinbarungen sind geschlossen. Die Pflichten zur Überprüfung der Unterauftragnehmer übernimmt die Geschäftsführung. Sie ist auch bei der Auswahl der beauftragten Firmen involviert.
	Wie wird die Löschung / Sperrung von personenbezogenen Daten am Ende der Aufbewahrungsfrist bei Unterauftragnehmern sichergestellt?	Festlegung durch Vertragsbindung, bei Wegfall des Zweckes ist ebenfalls eine Löschung der Daten indiziert.
3	**Verfügbarkeit und Belastbarkeit**	
3.1.	**Verfügbarkeitskontrolle**	
	Wie wird gewährleistet, dass die Datenträger vor elementaren Einflüssen (Feuer, Wasser, elektromagnetische Abstrahlung etc.) geschützt sind?	Gesicherte Daten sind räumlich getrennt von Produktivdaten.
	Welche Schutzmaßnahmen werden zur Bekämpfung von Schadprogrammen eingesetzt und wie wird deren Aktualität gewährleistet?	Ständig aktuelle Virenscanner und Spamfilter finden Einsatz. Die Systeme werden regelmäßig upgedatet.
	Wie wird sichergestellt, dass nicht mehr benötigte bzw. defekte Datenträger ordnungsgemäß entsorgt werden?	Physische Löschung bei funktionsfähigen Datenträgern und mechanische Zerstörung defekter Datenträger vor der Entsorgung.
3.2.	**Wiederherstellbarkeit**	

Nr.	Gebiet	Beschreibung
	Welche organisatorischen und technischen Maßnahmen werden getroffen, um auch im Schadensfall die Verfügbarkeit von Daten und Systemen schnellstmöglich zu gewährleisten? (rasche Wiederherstellbarkeit nach Art. 32 Abs.1 lit.c DS-GVO)	Eingerichtetes 2-stufiges Backup-Verfahren Wiederherstellung Datenstände der vergangenen 7 Tage auf Zuruf; Sicherung älterer Datenstände durch Einspielen von Bändern.
4.	**Verfahren zur regelmäßigen Überprüfung, Bewertung, Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO, Art. 25 Abs. 1 DS-GVO)**	
	Welche Verfahren gibt es zur regelmäßigen Bewertung/Überprüfung, um die Sicherheit der Datenverarbeitung zu gewährleisten (Datenschutz-Management)?	Die Geschäftsleitung überprüft regelmäßig und teilweise auch unangekündigt, die Einhaltung der technisch-organisatorischen Maßnahmen.
	Wie wird auf Anfragen bzw. Probleme reagiert (Incident-Response-Management)?	Einsatz eines Ticketsystems zweistufig (1st und 2nd Level); zusätzlich Telefonhotline und automatisierte Überwachung und Alarmierung
	Welche datenschutzfreundlichen Voreinstellungen gibt es (Art. 25 Abs. 2 DS-GVO)?	Keine Vorbelegung durch Haken; bei Anmeldung im System erfolgen optional keine Vorbelegungen; Benutzer muss dann die Anmeldeinformationen jeweils eintragen
4.1	**Auftragskontrolle**	
	Welche Vorgänge gibt es zur Weisung bzw. dem Umgang mit der Auftragsdatenverarbeitung (Datenschutz-Management)?	Das Vertragswerk wurde entsprechend den neuen Richtlinien zur Auftragsdatenverarbeitung gestaltet. Die Geschäfstleitung nimmt entsprechende Beratungs- und Kontrollpflichten wahr.

Stand: Februar 2023