Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

Vereinbarung

zwischen dem

Endkunden von Jumpian

– Verantwortlicher – nachstehend Auftraggeber genannt

und der

SYNNOTECH AG

– Auftragsverarbeiter – nachstehend Auftragnehmer genannt

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Der Gegenstand des Auftrags ergibt sich von dem Tag der Installation der Software Jumpian (https://www.jumpian.de/), auf den hier verwiesen wird (im Folgenden Leistungsvereinbarung).

(2) Dauer

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

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Art und Zweck der Verarbeitung personenbezogener sowie nicht personenbezogener Daten zur Vertragsabwicklung durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der Leistungsvereinbarung bzw. ergeben sich aus dem jeweiligen Support-Fall.

(2) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten können folgende Datenarten/-kategorien sein:

- Anwender-, Schüler-, Lehrerdaten
- Kommunikationsdaten:
  z. B. Telefon, E-Mail, etc.
- Personenstammdaten
- Planungs- und Steuerungsdaten:
  Zugriff auf Systeme des Auftraggebers nach Freigabe

- Vertragsabrechnungs- und Zahlungsdaten
- Vertragsstammdaten
- zur Verfügung gestellte Test- oder Produktivdaten

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen können umfassen:

- Ansprechpartner
- Auftraggeber/Lehrer
- Geschäftspartner des Auftraggebers: Die Daten für das Forderungsmanagement werden an den Dienstleister Digistore24 GmbH (vgl. 6. Unterauftragsverhältnisse) weitergegeben.
- Kollegen des Auftraggebers
- Schüler und Eltern
- Support für Endkunden

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.
(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen [Einzelheiten in Anlage 1].
(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.
(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt.
   - Als Datenschutzbeauftragte(r) ist beim Auftragnehmer Herr Christian Volkmer, Projekt 29 GmbH & Co. KG bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.
   - Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

b) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage 1].

d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

e) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

f) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

g) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören

Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.
(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen. Die Zustimmung erfolgt bei Bestellung auf https://www.jumpian.de/bestellung-digistore24.html.

Firma Unterauftragnehmer	Anschrift/Land	Leistung
Digistore24 GmbH	St.-Godehard-Straße 32 31139 Hildesheim	Übernahme des Forderungsmanagements

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.
(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.
(3) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen,
b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden,
c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen,
d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung,
e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.
(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.
(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

11. Haftung

Auf Art. 82 DS - GVO wird verwiesen.

SYNNO TECH
Hermann-Köhl-Straße 2a
93049 Regensburg
Phone: +49 941 297 88 30
www.synnotech.de

Unterschrift Auftraggeber	Unterschrift Auftragnehmer
Endkunde von Jumpian	SYNNOTECH AG
Ort, Datum	Regensburg, zum 25.05.2018 Ort, Datum

Anlage 1 – Technische und organisatorische Maßnahmen (TOM)

Nr.	Gebiet	Beschreibung
0	**Organisation**	
	Wie ist die Umsetzung des Datenschutzes organisiert?	Ein externer Datenschutzbeauftragter wird zur Wahrnehmung der Beratungs- und Kontrollfunktionen eingesetzt.
	Nennen Sie uns bitte den Namen und die Kontaktdaten Ihres Datenschutzbeauftragten.	Herrn Christian Volkmer Projekt 29 GmbH & Co. KG Ostengasse 14 93047 Regensburg Tel.: 0941 2986930 Fax: 0941 29869316 E-Mail: anfragen@projekt29.de Internet: www.projekt29.de
	Welche organisatorischen Maßnahmen wurden getroffen, damit die Verarbeitung personenbezogener Daten gesetzeskonform erfolgt?	Gelebte Prozesse werden in Schriftform dokumentiert.
	Wie stellen Sie sicher, dass die internen Prozesse gemäß den aktuellen Datenschutzbestimmungen ablaufen und regelmäßig geprüft werden?	Verarbeitungsverzeichnisse sind zum Teil über Qualitätsmanagement erstellt und werden über die DS-GVO überarbeitet.
	In welcher Form werden die Mitarbeiter auf die Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen geschult, die für diese Verarbeitung in Anwendung kommen?	Jährliche Schulung, neue Mitarbeiter im Rahmen der Einarbeitung und Sensibilisierung durch Datenschutz-Newsletter.
	Sind die Verarbeitungen hinsichtlich datenschutzrechtlicher Zulässigkeit dokumentiert?	Diese werden gerade erstellt.
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 Gebäude ist mit einer Sicherheits-Schließanlage ausgerüstet.
	Wie werden die Räume / Büros, in denen die Verarbeitung stattfindet, vor unbefugtem Zutritt gesichert?	Die Räume werden ebenfalls durch das Sicherheitsschließsystem gesichert.
	Wie werden die Verarbeitungsanlagen vor unbefugtem Zugriff geschützt?	passwortgeschützt, selbst sperrend

Nr.	Gebiet	Beschreibung
	Wie werden die umgesetzten Zutrittskontrollmaßnahmen auf Tauglichkeit geprüft?	Im Rahmen der Kontrollen durch den externen Datenschutzbeauftragten werden auch die Zutrittskontrollmaßnahmen überprüft.
1.2	**Zugangskontrolle**	
	Wie erfolgt die Vergabe von Benutzerzugängen?	Durch die Geschäftsleitung, schriftliche Anweisung an die IT.
	Wie wird die Gültigkeit von Benutzerzugängen überprüft?	Bisher gab es keine Protokollauswertungen.
	Wie werden Benutzerzugänge inkl. Antragstellung, Genehmigungsverfahren etc. dokumentiert?	E-Mail von Geschäftsleitung an Admin. Wird in elektronischer Personalakte aufbewahrt.
	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?	Es gibt zwei Administratoren.
	Ist ein Zugriff auf die Systeme / Anwendungen von außerhalb des Unternehmens möglich (Heimarbeitsplätze, Dienstleister etc.) und wie ist der Zugang gestaltet?	Zugriff auf den Sourcecode und E-Mails ist mittels Zugangsdaten möglich (interne und externe Mitarbeiter). Sonst keine Dienstleister.
1.3	**Zugriffskontrolle**	
	Wie wird erreicht, dass Passwörter nur dem jeweiligen Benutzer bekannt sind?	Vom Admin zufällig generiertes Passwort.
	Welche Anforderungen werden an die Komplexität von Passwörtern gestellt?	8 Zeichen: Großbuchstaben, Kleinbuchstaben und zwei Zahlen
	Wie wird gewährleistet, dass der Benutzer sein Passwort regelmäßig ändern kann / muss?	keine Passwortänderung verpflichtend
	Welche organisatorischen Vorkehrungen werden zur Verhinderung von unberechtigten Zugriffen auf personenbezogene Daten am Arbeitsplatz getroffen?	internes Reinigungspersonal mit Verschwiegenheitsverpflichtung Bildschirm sperren GL (HR): Büros sind zusätzlich verschlossen
	Wie wird sichergestellt, dass Zugriffsberechtigungen anforderungsgerecht und zeitlich beschränkt vergeben werden?	Tätigkeiten werden anhand der Aufgaben- und Zuständigkeitsmatrix überprüft und entsprechende Rechte vergeben / entzogen. Beim Ausscheiden ist durch ein Prozess die komplette Zugangsregelung sichergestellt.

Nr.	Gebiet	Beschreibung
	Wie erfolgt die Dokumentation von Zugriffsberechtigungen?	Zugriffskontrolle des Sourcecodes/Intranets über LDAP. Über Microsoft Partner Plattform werden Zugriffe der Microsoft Produkte geregelt. Die restlichen Lizenzen sind am internen Netzlaufwerk hinterlegt.
	Wie wird sichergestellt, dass Zugriffsberechtigungen nicht missbräuchlich verwendet werden?	siehe vorherige Frage (MS / LDAP)
	Wie lange werden Protokolle aufbewahrt? Wer hat Zugriff auf die Protokolle und wie oft werden sie ausgewertet?	Zugriff hat IT. Sporadische Auswertung => Maximale Speicherung: 6 Wochen
1.4	**Trennungskontrolle**	
	Wie wird sichergestellt, dass Daten, die zu unterschiedlichen Zwecken erhoben wurden, getrennt voneinander verarbeitet werden?	Server im Haus: Projektdaten, fachliche Anforderungen Trennung durch Ordnerstruktur
1.5	**Pseudonymisierung**	
	Welche organisatorischen Maßnahmen wurden getroffen, damit die Verarbeitung personenbezogener Daten gesetzeskonform erfolgt?	Trifft aufgrund der Unternehmensgröße bei uns nicht zu.
	Wie werden personenbezogene Daten verarbeitet /aufbewahrt, sodass diese nicht den betroffenen Personen zugeordnet werden können?	siehe vorherige Frage
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?	Elektronische Weitergabe verschlüsselt an den Steuerberater
	Werden Verschlüsselungssysteme bei der Weitergabe von personenbezogenen Daten eingesetzt und wenn ja, welche?	Zip-Verschlüsselung
	Wie wird die Weitergabe personenbezogener Daten dokumentiert?	Gesendete Mail wird im separaten Ordner aufbewahrt. 12 Monate Haltefrist

Nr.	Gebiet	Beschreibung
	Wie wird der unberechtigte Abfluss von personenbezogenen Daten durch technische Maßnahmen beschränkt?	keine Beschränkung möglich, da Mitarbeiter Entwickler sind
	Gibt es ein Kontrollsystem, das einen unberechtigten Abfluss von personenbezogenen Daten aufdecken kann?	nein
2.2.	**Eingabekontrolle**	
	Welche Maßnahmen werden ergriffen, um nachvollziehen zu können, wer wann und wie lange auf Applikationen zugegriffen hat?	Buchhaltung und Personaldaten werden nur im Bereich der Geschäftsleitung verarbeitet. Sonstige Applikationen enthalten keine personenbezogenen Daten. Änderungsverfolgung in YouTrack; in MS Office nicht möglich
	Wie ist nachvollziehbar, welche Aktivitäten auf den entsprechenden Applikationen durchgeführt wurden?	Gar nicht, da keine Mitarbeiter mit diesen Aufgaben betraut sind.
	Welche Maßnahmen werden ergriffen, damit die Verarbeitung durch die Mitarbeiter nur gemäß der Weisung des Auftraggebers erfolgen kann?	Verpflichtungserklärung gemäß DS-GVO der Mitarbeiter zum gesetzeskonformen Umgang mit personenbezogenen Daten angewiesen. Außerdem wird ein Verarbeitungsverzeichnis zum Support/zur Entwicklung erstellt und intern verwendet.
	Welche Maßnahmen werden getroffen, damit auch Unterauftragnehmer ausschließlich im vereinbarten Umfang personenbezogene Daten des Auftraggebers verarbeiten?	Dies wird im ADV geregelt.
	Wie wird die Löschung / Sperrung von personenbezogenen Daten am Ende der Aufbewahrungsfrist bei Unterauftragnehmern sichergestellt?	siehe vorherige Frage
3	**Verfügbarkeit und Belastbarkeit**	
3.1.	**Verfügbarkeitskontrolle**	
	Welche organisatorischen und technischen Maßnahmen werden getroffen, um auch im Schadensfall die Verfügbarkeit von Daten und Systemen schnellstmöglich zu gewährleisten?	tägliches Backup auf intern verschlüsselte Festplatte (interner Server und vom externen Rechenzentrum) physikalische Aufbewahrung außerhalb des Unternehmens

Nr.	Gebiet	Beschreibung
	Wie wird gewährleistet, dass die Datenträger vor elementaren Einflüssen (Feuer, Wasser, elektromagnetische Abstrahlung etc.) geschützt sind?	Es gibt keinen besonderen Schutz (zwei Laptops).
	Welche Schutzmaßnahmen werden zur Bekämpfung von Schadprogrammen eingesetzt und wie wird deren Aktualität gewährleistet?	Firewall, Virenschutz (Bitdefender)
	Wie wird sichergestellt, dass nicht mehr benötigte bzw. defekte Datenträger ordnungsgemäß entsorgt werden?	Platten werden als defekt markiert und in einem separaten Behältnis in einem abgeschlossenen Raum aufbewahrt.
3.2.	**Wiederherstellbarkeit**	
	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)	durch Spiegelung und Backup
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)?	DSB überprüft regelmäßig die TOM's.
	Wie wird auf Anfragen bzw. Probleme reagiert (Incident-Response-Management)?	Wird im Rahmen des Datenschutz-Prozesses definiert.
	Welche datenschutzfreundlichen Voreinstellungen gibt es (Art. 25 Abs. 2 DS-GVO)?	Es werden nur minimale Identifikationsmerkmale gespeichert.
4.1	**Auftragskontrolle**	
	Welche Vorgänge gibt es zur Weisung bzw. dem Umgang mit der Auftragsdatenverarbeitung (Datenschutz-Management)?	Das Vertragswerk gemäß den Richtlinien zur ADV wird gerade geschlossen, von DSB begleitet und kontrolliert.