Vereinbarung zur Verarbeitung personenbezogener Daten im Auftrag

zwischen der [Name der Schule/ Einrichtung/Organisation]
- nachstehend Auftraggeber genannt –

und der bettermarks GmbH
- nachstehend Auftragnehmer genannt –

§ 1 Gegenstand und Dauer der Vereinbarung

(1) Der Auftrag umfasst folgende Arbeiten des Auftragsnehmers: Bereitstellung, Betrieb und Verfügbar halten des online-Lernsystems bettermarks und der dort gespeicherten Daten.
(2) Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO.
(3) Dauer des Auftrags
Die Laufzeit dieses Vertrages richtet sich nach der Laufzeit des Nutzungsvertrages, den Auftraggeber und Auftragnehmer über die Nutzung der Lernplattform bettermarks schließen. Dies gilt auch, wenn Auftraggeber bettermarks über eine Landeslizenz nutzen.

§ 2 Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen

Die Lernplattform bettermarks unterstützt Lehrende beim Mathematikunterricht. Es ist ein vollständig digitales adaptives Online-Lernsystem. Es zielt auf den individuellen Lernprozess der Lernenden ab und bietet Rückmeldungen, Erkennung systematischer Fehler und verschiedene Arten von Übungen.

1. Lehrende können einer Klasse bzw. Gruppe oder einzelnen Lernenden Übungsserien zuweisen. Die Lehrenden können den individuellen Fortschritt aller Lernenden im Detail verfolgen – hierfür werden Auswertungen und Berichte bereitgestellt – es ist aber auch möglich, die tatsächlich eingegebenen Lösungen einzusehen.
2. Die Lernenden können Übungsserien, die ihnen zugewiesen wurden, lösen. Zusätzlich lassen sich die von bettermarks bereit gestellten Übungsserien bearbeiten. Dies ist von jedem Ort mit Internetzugang aus möglich und setzt neben ebendiesem Internetzugang nur ein aktuelles Endgerät (Smartphone, Tablet, PC) voraus. Da es sich bei bettermarks um eine SaaS-Lösung (Software-as-a-Service) handelt, können Lernende eine Übungsserie auf einem Computer starten und unterwegs auf einem Smartphone und dann zuhause auf einem privaten Gerät beenden.
3. Der Auftragnehmer hat die didaktische Qualität des Lernsystems laufend zu überprüfen und gegebenenfalls anzupassen. Dazu führt er interne Statistiken und nutzt auch anonymisierte Kopien der Daten.
4. In Situationen, wo der Auftraggeber bettermarks NICHT über eine Landeslizenz nutzt, können Lehrende eine Schul-/Klassenlizenz über die bettermarks eigene Lizenzverwaltung erwerben.

(1) Kategorien betroffener Personen gemäß der Definition von Art. 4 Nr. 1 DSGVO
   a. Lehrende
   b. Lernende
(2) Art der personenbezogenen Daten gemäß der Definition von Art. 4 Nr. 1
   a. Für die Benutzerkonten der Lernenden werden verarbeitet:
      i. IP-Adresse
      ii. Authentifizierungstoken
      iii. Browserinformationen
      iv. Eine pseudonyme bettermarks Benutzer-ID
      v. Ein Benutzername
      vi. Ein Passwort (wird lediglich als Hash-Wert gespeichert)
      vii. Zuordnung zu einer Schule/Einrichtung/Organisation.
      viii. Zuordnung zu einer Gruppe oder Klasse oder auch mehreren
   b. Für die Benutzerkonten der Lehrenden werden verarbeitet:

i. IP-Adresse
ii. Authentifizierungstoken
iii. Browserinformationen
iv. Eine pseudonyme bettermarks Benutzer-ID
v. Als Benutzername die E-Mail-Adresse
vi. Ein Passwort (wird lediglich als Hash-Wert gespeichert)
vii. Vor- und Nachname
viii. Zuordnung zu einer Schule/Einrichtung/Organisation.
ix. Zuordnung zu einer Gruppe oder Klasse bzw. auch mehreren.

c. Wenn Lernende und Lehrende bettermarks verwenden, werden folgende Lernstandsdaten verarbeitet:
   i. Aufgaben (von Lehrenden zugewiesene Übungsserien)
   ii. Aktivitäten (was haben Lernende wann und mit welchem Ergebnis eingegeben)
   iii. Empfehlungen (ausgehend von Fehlern empfiehlt bettermarks neue Serien)
d. Wenn Lehrende die bettermarks eigene Lizenzverwaltung verwenden, so werden folgende Daten verarbeitet:
   i. Kontaktdaten des Lehrenden
   ii. Rechnungsdaten der Schule/Schulträger o.ä.

(3) Fristen für die Löschung der verschiedenen Datenkategorien:
Alle inaktiven Benutzerkonten werden vollständig und unwiederbringlich gelöscht, wenn das Schuljahr beendet ist, in dem der Account inaktiv war. Inaktivität ist definiert als ein ganzes Schuljahr ohne Aktivität bzw. Anmeldung am Benutzerkonto. Mit dem Benutzerkonto werden alle personenbezogenen und personenbeziehbaren Daten gelöscht. Die Löschung schließt die konkreten Eingaben der Lernenden ein.
Rechnungsdaten werden entsprechend der gesetzlichen Fristen gelöscht.

§ 3 Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber ist berechtigt, sich wie unter §4 Abs. 3 festgelegt vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.
(2) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

§ 4 Rechte und Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers.
(2) Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DSGVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen.
(3) Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber - grundsätzlich nach Terminvereinbarung - berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort.
(4) Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet.

(5) Der Auftragnehmer ist verpflichtet, alle Anfragen gem. Artikel 12 bis 22 DSGVO, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten

§ 5 Verpflichtung des Auftragnehmers zur Information des Auftragsgebers (Art. 28 Abs. 3 S. 2 lit. a DSGVO)

Der Auftragnehmer verarbeitet die Auftraggeber-Daten gemäß den Weisungen des Auftraggebers, sofern der Auftragnehmer nicht gesetzlich zu einer anderweitigen Verarbeitung verpflichtet ist. In letzterem Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Gesetz eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

§ 6 Verpflichtung des Auftragnehmers zur Information des Auftraggebers, wenn er der Auffassung ist, dass eine Weisung gegen datenschutzrechtliche Bestimmungen verstößt (Art. 28 Abs. 3 S. 3 DSGVO)

Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen diesen Vertrag oder das geltende Datenschutzrecht verstößt, ist er nach einer entsprechenden Mitteilung an den Auftraggeber berechtigt, die Ausführung der Weisung bis zu einer Bestätigung der Weisung durch den Auftraggeber auszusetzen. Die Parteien stimmen darin überein, dass die alleinige Verantwortung für die weisungsgemäße Verarbeitung der Auftraggeber-Daten beim Auftraggeber liegt

§ 7 Regelung, dass eine Verarbeitung Daten des AG durch AN grundsätzlich in EU/EWR stattfindet und eine Drittstaatenübermittlung nur mit vorheriger Zustimmung des AG zulässig ist (Art. 28 Abs. 3 S. 2 lit. a DSGVO)

Die Verarbeitung der Auftraggeber-Daten durch den Auftragnehmer findet grundsätzlich innerhalb der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) statt.

§ 8 Verpflichtung des AN, dem Unterauftragnehmer dieselben Datenschutzpflichten wie im Hauptvertrag nach Art. 28 DSGVO aufzuerlegen (Art. 28 Abs. 3 S. 2 lit. d i.V.m. Art. 28 Abs. 4 DSGVO)

Der Vertrag zwischen dem Auftragnehmer und dem weiteren Auftragsverarbeiter muss letzterem dieselben Pflichten auferlegen, wie sie dem Auftragnehmer kraft dieses Vertrages obliegen. Die Parteien stimmen überein, dass diese Anforderung erfüllt ist, wenn der Vertrag ein diesem Vertrag entsprechendes Schutzniveau aufweist bzw. dem weiteren Auftragsverarbeiter die in Art. 28 Abs. 3 DSGVO festgelegten Pflichten auferlegt sind.

§ 9 Unterauftragsverhältnisse mit weiteren Auftragsverarbeitern (Art. 28 Abs. 3 Satz 2 lit. d DSGVO)

Der Auftraggeber erteilt dem Auftragnehmer hiermit eine allgemeine schriftliche Genehmigung zur Beauftragung von weiteren Auftragsverarbeitern zur Verarbeitung von personenbezogenen Daten. Die Liste der beauftragten Auftragsverarbeiter ist Anlage 1 zu entnehmen. Der Auftragnehmer informiert den Auftraggeber über jede beabsichtigte Änderung bezüglich der Hinzuziehung oder Ersetzung anderer Auftragsverarbeiter. Der Auftraggeber hat hierauf die Möglichkeit innerhalb von 4 Wochen der Änderung zu widersprechen.

§ 10 Technische und organisatorische Maßnahmen (insbesondere Art. 28 Abs. 3 Satz 2 lit. c und e DSGVO)

Der Auftragnehmer sorgt unter Einhaltung der in Anlage 2 hinterlegten technischen und organisatorischen Maßnahmen dafür, dass die Verarbeitung der personenbezogenen Daten den Vorgaben des Art. 32 DSGVO entspricht. Die technischen und organisatorischen Maßnahmen sind dem Stand der Technik anzupassen. Dabei wird sichergestellt, dass das bestehende Schutzniveau der Maßnahmen zur Datensicherheit des Auftragnehmers bei Änderungen nicht unterschritten wird.

Wesentliche Änderungen der technischen und organisatorischen Maßnahmen teilt der Auftragnehmer dem Auftraggeber mit.

§ 11 Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags, Art. 28 Abs. 3 Satz 2 lit. g DSGVO

Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder zu löschen oder zurückzugeben und die vorhandenen Kopien zu löschen, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

§ 12 Sonstiges

(1) Für Nebenabreden oder Ergänzungen dieses Vertrages ist grundsätzlich die Schriftform erforderlich, was auch in einem elektronischen Format erfolgen kann.
(2) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.
(3) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.
(4) Für diesen Vertrag gilt deutsches Recht mit Ausnahme der Bestimmungen des internationalen Privatrechts.

.....	.....
Ort, Datum	Unterschrift des Auftraggebers
Berlin, 14.12.23	
Ort, Datum	Unterschrift des Auftragnehmers

Anlagen

- Anlage 1: Liste der Auftragsverarbeiter und Dienstleister
- Anlage 2: Technische und Organisatorische Maßnahmen

Anlage 1

Auftragsverarbeiter, die bettermarks bei der Erbringung der vereinbarten Leistungen hinzuzieht (Art. 28 Abs. 3 Satz 2 Lit. D DSGVO)

Auftragnehmer	Teilleistung	Ort der Datenverarbeitung
IONOS SE Elgendorfer Str. 57 56410 Montabaur	Hosting der bettermarks-Systeme	Deutschland
Commehr GmbH Nürnberger Str. 38 10777 Berlin	IT-Dienstleister, Wartung der Geräte im bettermarks-Büro	Deutschland
Cloudflare GmbH Rosental 7 80331 München	IT-Sicherheits-Dienstleister, Schutz der bettermarks Plattform	Deutschland
Brevo GmbH Köpenicker Straße 126 10179 Berlin	Versand von Rechnungen für Lizenzen per Email an Schulen/Organisationen	Deutschland
RAIDBOXES GmbH Friedrich-Ebert-Straße 7 48153 Münster	Generierung von Rechnungen für Lizenzen an Schulen/ Organisationen	Deutschland
visual4 GmbH Schreiberstr. 27 70199 Stuttgart	Betrieb des CRM-Systems zur Verwaltung von Lizenzhaltern. (Schulen&Lehrende)	Deutschland

Dienstleister, die keine Auftragsverarbeiter sind

Auftragnehmer	Teilleistung	Ort der Datenverarbeitung
AMAZON WEB SERVICES EMEA SARL Two Park Place, Hatch Street, Dublin 2, Ireland	Verarbeitung faktisch anonymer Lernereignisse	Deutschland
Mixpanel, Inc. 1 Front Street, Floor 28, San Francisco, California 94111, US	Interne Statistik faktisch anonymer Nutzer-Ereignisse	Europa

Anlage 2

Technische und organisatorische Maßnahmen (TOM) i.S.d. Art. 32 DSGVO

Angaben über die technischen und organisatorischen Maßnahmen (kurz TOM) des oben benannten Unternehmens nach Art. 32 DSGVO. Organisationen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben technische und organisatorische Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zum angestrebten Schutzzweck steht.

Das oben genannte Organisation erfüllt diesen Anspruch durch folgende Maßnahmen:

Vorwort

Der Zugriff auf Systeme, in denen personenbezogene Daten verarbeiten werden, kann aus den folgenden Bereichen stattfinden:

1. Büro der Bettermarks GmbH (Skalitzer Str. 85-86, 10997 Berlin)
2. Mobiles Arbeiten der Mitarbeitenden
3. Bei Unterauftragsverarbeitern (siehe Anlage 3)

Neben den nachfolgend dargestellten technischen und organisatorischen Maßnahmen wird das mobile Arbeiten von Mitarbeitenden durch eine spezielle Richtlinie geregelt.

Die Auswahl der Unterauftragnehmer erfolgt unter Beachtung der Vorgaben der DSGVO sowie dem Bestehen einer gültigen ISO 27001 Zertifizierung.

Vertraulichkeit gem. Art. 32 Abs. 1 DSGVO

1. Zutrittskontrolle

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Schließsystem mit Transpondern	☒ Schlüsselregelung / -liste / -verwaltung
☒ Türen mit Knauf an Außenseite	☒ Dokumentation Schlüsselausgabe
☒ Klingelanlage	☒ Dokumentation Schlüsselrückgabe

2. Zugangskontrolle

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Login mit Benutzername + Passwort	☒ Richtlinie zulässige Hard- und Software
☒ 2-Faktor-Authentifizierung	☒ Benutzerberechtigungskonzept
☒ Gehärtete Serversysteme	☒ Verwalten von Benutzerprofilen (Regelung)
☒ Anti-Virus-Software Notebooks	☒ Richtlinie „Sicheres Passwort“
☒ Web-Application Firewall-System	☒ Richtlinie „Mobiles Arbeiten“
☒ Firewall-System	☒ Allg. Richtlinie Datenschutz und / oder IT-Sicherheit
☒ Intrusion Detection Systeme	☒ Passwortmanager
☒ Intrusion Prevention Systeme	
☒ Mobile Device Management	
☒ Einsatz VPN bei Remotezugriffen	
☒ Verschlüsselung von Datenträgern	
☒ Verschlüsselung Mobilen Geräten (Notebooks, Tablets, Surface)	
☒ BIOS-Schutz (separates Passwort)	
☒ Sperre externer Schnittstellen (USB)	
☒ Automatische Desktopsperre mit Kennwort	

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Verschlüsselung von Notebooks / Tablet, Datenträgern	
☒ Netzwerktrennung Produktivsystem, Testsysteme, Produktion (Maschinensteuerung)	

3. Zugriffskontrolle

3.1. Benutzer sind Sicherheitsgruppen zugeordnet. Über diese Sicherheitsgruppen werden Berechtigungen für die Zugriffe auf Ressourcen erteilt. Die Anmeldung an einem Benutzerkonto setzt Multifaktorauthentifizierung voraus.

3.2. Alle Mitarbeitenden greifen mit ihren persönlichen Konten auf die Systeme zu. Die Nutzung technischer Konten ist nicht gestattet.

3.3. Wenn Mitarbeitende das Unternehmen verlassen, werden die zugehörigen Konten gesperrt und anschließend gelöscht. Alle Konten werden regelmäßig überprüft und Konten, die zu nicht aktiven Mitarbeitenden gehören, werden gelöscht oder gesperrt.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten	☒ Rollenbasiertes Berechtigungskonzept
	☒ Bedarfsgerechtes Zugriffskonzept
	☒ Zentrale Verwaltung der Benutzerrechte durch IT
	☒ Minimale Anzahl an Administratoren
	☒ Checkliste für Mitarbeiteraustritt
	☒ Administratoren haben zusätzlich einen User-Account mit „nur“ einfachen Benutzerrechten (Internet- und E-Mail-Nutzung nur über User-Account)

4. Trennungskontrolle

4.1. Entwicklungs-, Test-, Abnahme- und Produktionsumgebung sind streng voneinander getrennt.

4.2. Produktionsdaten (Benutzernamen, Passwörter, etc.) und persönliche Daten werden nicht in Entwicklungs- und Testumgebungen verwendet.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Trennung von Produktiv- und Testumgebung	☒ Steuerung über Berechtigungskonzept
☒ Sandboxing (Testumgebung)	☒ Festlegung von Datenbankrechten

5. Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

5.1. bettermarks verarbeitet nur nicht unmittelbar identifizierende Daten der Nutzenden. Im Falle der pseudonymen Benutzer-IDs hat bettermarks keinen Zugriff auf die Zuordnungsdaten.

5.2. Zusätzlich wird durch die Verwendung eines Reverse-Proxys der Zugriff von bettermarks auf die IP-Adresse des Nutzenden verhindert. Für Situationen, wo die bettermarks-Anwendung über den Reverse-Proxy eines Integrationspartners eingebunden wird, sind folgende Maßnahmen getroffen: Es gibt einen automatischen Mechanismus, der bestimmt, welche Domänen von der bettermarks-Anwendung auf dem Continuous-Integration-System verwendet werden. Das Integrationsteam informiert dann den Partner rechtzeitig, bevor die neue Domäne in Produktion verwendet wird. Dies sorgt dafür, dass bei Nutzung der bettermarks-Anwendung alle Datenpakete mit einer neutralen IP-Adresse durch den Auftragnehmer empfangen werden. Wenn eine neue Domäne auftaucht, wird eine Benachrichtigung an das Integrations- und Data-Privacy-Team gesendet.

5.3. Testdaten sind stets anonym.

5.4. Die zur didaktischen Qualitätssicherung verwendeten Systeme zur Erstellung interner Statistiken sind von der Produktionsumgebung getrennt. Bei der Erstellung von anonymisierten Kopien dieser Daten werden die pseudonymen Benutzer-IDs mit einem transienten Einmal-Zufallsschlüssel verhasht.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Trennung der pseudonymen Daten und der Zuordnungsdaten	☒ Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren

Integrität (Art. 32 Abs. 1 lit. b DSGVO)

6. Weitergabekontrolle

6.1. Der gesamte externe Datenverkehr erfolgt verschlüsselt (nach dem Stand der Technik).

6.2. Die physisch gespeicherten Daten sind nach dem Stand der Technik verschlüsselt.

6.3. Der Zugriff auf die bettermarks-Anwendung und die Änderung persönlicher Daten werden protokolliert. Die Protokollierung ist nur autorisierten Personen zugänglich.

6.4. Die gesetzlichen Aufbewahrungsfristen für personenbezogene Daten, Loggingdaten und Lernstandsdaten usw. werden eingehalten.

6.5. Wenn ein Benutzerkonto ein Schuljahr lang keine Aktivität gezeigt hat (kein Login), so werden die dazugehörigen personenbezogenen Daten unwiederbringlich gelöscht.

6.6. Auf Weisung des Verantwortlichen erfolgt eine Löschung, Sperrung oder Korrektur personenbezogener Daten.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Einsatz von VPN	☒ Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen
☒ Protokollierung der Zugriffe und Abrufe	☒ Weitergabe in anonymisierter oder pseudonymisierter Form
☒ Bereitstellung über verschlüsselte Verbindungen wie sftp, https	☒ Löschkonzept zur Löschung von Daten und Vernichtung von Datenträgern
☒ Nutzung von Signaturverfahren	
☒ Missbrauchsschutz von USB-Schnittstellen durch: Verschlüsselung mobiler Datenträger Sperrung der USB-Ports	

7. Eingabekontrolle

7.1. Es erfolgt eine Prüfung der Eingaben und Anfragen auf permanent aktualisierte Angriffsmuster. Es werden automatisch Gegenmaßnahmen eingeleitet, sofern auffällige Eingaben oder Anfragen erfolgen.

7.2. Login–Aktivitäten von Nutzenden und Änderungen an personenbezogenen Daten werden geloggt, sodass Logins und Veränderung nachvollzogen werden können.

7.3. Es ist rückverfolgbar, an welchen Systemkomponenten welche Änderungen wann und mit welchem Benutzerkonto durchgeführt wurden. Durch die Rückverfolgbarkeit ist es möglich, die Änderungen rückgängig zu machen.

7.4. Sicherheits- und Softwareupdates werden nach Veröffentlichung schnellstmöglich und weitestgehend automatisiert eingespielt.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	☒ Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können
☒ Manuelle oder automatisierte Kontrolle der Protokolle	☒ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch Individuelle Benutzernamen (nicht Benutzergruppen)
	☒ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
	☒ Klare Zuständigkeiten für Löschungen (Lösch-Konzept)

8. Eingabekontrolle

8.1. Es erfolgt eine Prüfung der Eingaben und Anfragen auf permanent aktualisierte Angriffsmuster. Es werden automatisch Gegenmaßnahmen eingeleitet, sofern auffällige Eingaben oder Anfragen erfolgen.

8.2. Login–Aktivitäten von Nutzenden und Änderungen an personenbezogenen Daten werden geloggt, sodass Logins und Veränderung nachvollzogen werden können.

8.3. Es ist rückverfolgbar, an welchen Systemkomponenten welche Änderungen wann und mit welchem Benutzerkonto durchgeführt wurden. Durch die Rückverfolgbarkeit ist es möglich, die Änderungen rückgängig zu machen.

8.4. Sicherheits- und Softwareupdates werden nach Veröffentlichung schnellstmöglich und weitestgehend automatisiert eingespielt.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	☒ Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können
☒ Manuelle oder automatisierte Kontrolle der Protokolle	☒ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch Individuelle Benutzernamen (nicht Benutzergruppen)
	☒ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
	☒ Klare Zuständigkeiten für Löschungen (Lösch-Konzept)

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

9. Verfügbarkeitskontrolle

9.1. Die Zahl der Nutzenden, der anfallende Netzwerkverkehr und die Auswirkungen auf die Systeme und der Ressourcenverbrauch werden fortlaufend und automatisch überwacht. Die Kapazität der Systeme und die Hardware werden dabei so dimensioniert, dass das Doppelte der täglich gemessenen Spitzenbelastung verarbeitet werden kann. Zudem sind Warnschwellen für die Ressourcenauslastungen definiert. Bei einer Überschreitung werden Alarme ausgelöst. Wenn eine Überlastung festgestellt wird, werden kurzfristig zusätzliche Kapazitäten zugeschaltet. bettermarks führt proaktiv Leistungstests durch, um die Auswirkungen von Architekturänderungen auf den Ressourcenverbrauch zu prüfen.

9.2. Alle relevanten Systemkomponenten sind redundant ausgelegt.

9.3. Während der Design-Phase der Systeme wurden die Abhängigkeiten der einzelnen Komponenten betrachtet und die Auswirkungen von Ausfällen einzelner Teilsysteme minimiert. Zudem werden die Verfügbarkeit und Ausfallsicherheit der relevanten Komponenten regelmäßig getestet. Es gibt einen mehrstufigen aktiven Schutz gegen (D)DoS-Attacken.

9.4. Sicherheitspatches, Updates der Systemkomponenten, sowie Erneuerung von Zertifikaten werden regelmäßig eingespielt. Kritische Sicherheitspatches werden zeitnah installiert.

9.5. Die verantwortlichen Mitarbeitenden sind sich der Bedrohungen der Verfügbarkeit bewusst. Mit entsprechenden Prozessen wird auf Bedrohungen reagiert.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Einsatz/Nutzen von Cloud-Systemen in externen Rechenzentren	☒ Backup & Recovery-Konzept
	☒ Kontrolle der Sicherungsvorgänge
	☒ Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse

10. Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)

10.1. Es erfolgt ein regelmäßiges, automatisiertes Backup der Datenbanken. Das maximale Alter der geretteten Daten im Falle einer Katastrophen- bzw. Notfallwiederherstellung (RPO / Recovery Point Objective) beträgt 30 Minuten. Zudem wird regelmäßig ein Datenwiederherstellungstest mit einem RTO (Wiederherstellungszeitziel) von weniger als 24 Stunden durchgeführt.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Jederzeit eine aktuelle Datensicherung	☒ Regelmäßige Kontrollen und Trainings zur System- und Datenwiederherstellung
	☒ Es werden Ersatzsysteme (Hardware) vorgehalten
	☒ Restorekonzept inkl. wichtiger Telefonnummern die im Bedarfsfall benötigt werden (Notfallkontakt)

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

11. Datenschutz-Management

11.1. Es wurde eine Risiko- / Gefahrenanalyse der Anwendung durchgeführt.

11.2. Es werden regelmäßig Penetrationstests durchgeführt, um Schwachstellen zu identifizieren und zu beheben.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z.B. Wiki, Intranet etc.)	☒ Externer Datenschutzbeauftragter Johannes Endres c/o Althammer & Kill GmbH & Co. KG Roscherstr. 7, 30161 Hannover kontakt-dsb@althammer-kill.de
☒ Sicherheitszertifizierung des RZ nach ISO 27001	☒ Mitarbeitenden geschult und auf Vertraulichkeit verpflichtet
☒ Dokumentiertes Sicherheitskonzept	☒ Regelmäßige Sensibilisierung der Mitarbeitenden (mindestens 1x jährlich)
☒ Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird regelmäßig durchgeführt	☒ Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach
	☒ Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden

12. Incident-Response-Management

12.1. Die Verfügbarkeit und die Nutzung der wesentlichen Komponenten werden fortlaufend überwacht.

12.2. Entdeckt das Monitoring-System Vorfälle, so beginnt ein strukturierter Benachrichtigungs- und Behebungsprozess. In gravierenden Fällen wird ein sogenannter Betriebsvorfall („Incident“) ausgelöst. Die Regeln dafür stellen sicher, dass das Problem zügig, effizient und mit allen benötigten Ressourcen behoben werden kann.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Einsatz von Firewall und regelmäßige Aktualisierung	☒ Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflichten und -fristen gegenüber Aufsichtsbehörden - 72 Std.)
☒ Einsatz von Spamfilter und regelmäßige Aktualisierung	☒ Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
☒ Einsatz von Virenscanner und regelmäßige Aktualisierung	☒ Einbindung des Datenschutzbeauftragten in Sicherheitsvorfälle und Datenpannen
☒ Intrusion Detection System (IDS)	☒ Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem
☒ Intrusion Prevention System (IPS)	☒ Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen
☒ regelmäßige Sensibilisierung der Mitarbeiter in Datenschutz bzw. Datensicherheit	

13. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO);

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	☒ Dokumentation in Datenschutzrichtlinie, Datenschutz-Handbuch, IT-Security-Richtlinie
☒ Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen	☒ Software und Hardware ist von Grund auf so konzipiert und entwickelt, dass relevante Datenschutzmaßnahmen von Anfang an berücksichtigt werden
☒ Für Webseitenbenutzer werden benutzerfreundliche Einstellungsmöglichkeiten zum Schutz ihrer Privatsphäre eingesetzt (für Cookie-, und Tracking-Einsatz)	☒ Einhaltung der Datenschutzgrundsätze ☒ Datenminimierung ☒ Sicherheit der Verarbeitung ☒ Pseudonymisierung ☒ Anonymisierung

14. Auftragskontrolle (Outsourcing an Dritte)

Technische Maßnahmen	Organisatorische Maßnahmen
	☒ Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
	☒ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten
	☒ Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU-Standard-Vertragsklauseln (siehe unten)
	☒ Schriftliche Weisungen an den Auftragnehmer
	☒ Verpflichtung der Mitarbeiter des Auftragnehmers zur Vertraulichkeit

Technische Maßnahmen	Organisatorische Maßnahmen
	☒ Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen der Bestellpflicht
	☒ Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
	☒ Regelung zum Einsatz weiterer Subunternehmer
	☒ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
	☒ Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus
	☒ Angemessenheitsbeschluss (gem. Art. 45 Abs. 3 DSVO)
	☒ Geeignete Garantien i. S. v. Art. 46 Abs. 2 DSGVO