Anlage 2.1
zur Anlage 2 zum Vertrag zum Erwerb des Deutschlandsemestertickets

Vereinbarung über die gemeinsame Verantwortlichkeit
nach Art. 26 der Datenschutz-Grundverordnung (DSGVO)

zwischen

der verfassten Studierendenschaft der Universität Potsdam
– vertreten durch den Allgemeinen Studierendenausschuss (AStA) –

(„**Vertragspartner**“)

und

der ViP Verkehrsbetrieb Potsdam GmbH
– vertreten durch die Geschäftsführung –

(„**Verkehrsunternehmen**“)

und

der Barnimer Busgesellschaft mbH,
– vertreten durch die Geschäftsführung –

(„**BBG**“,
gemeinsam mit dem Vertragspartner und dem Verkehrsunternehmen „**Parteien**“ und einzeln auch „**Partei**“)

Präambel

Die Parteien haben den „Vertrag zum Erwerb des Deutschlandsemestertickets“ geschlossen („**Hauptvertrag**“). Ziel des Hauptvertrags ist es, den Studierenden ein grundsätzlich obligatorisches und kostenreduziertes Deutschlandticket für Studierende („**Deutschlandsemesterticket**“ oder „**DST**“) bereitzustellen, das digital als Online-Ticket ausgegeben wird. Der Beitrag für das DST werden mit den Semesterbeiträgen vom Vertragspartner eingezogen.

Dabei haben sich die Verkehrsunternehmen in Brandenburg, die Verträge zum Erwerb des Deutschlandsemestertickets mit Hochschulen bzw. Studierendenschaften im Land Brandenburg geschlossen haben („**vertragshaltende Verkehrsunternehmen**“), darauf verständigt,

dass für die vertragshaltenden Verkehrsunternehmen BBG mit der Digital H GmbH („**Dienstleister**") einen Vertrag über die Nutzung der Web-Applikation RIDECampus („**App**") schließt und dem Dienstleister die Ausstellung des DST überträgt. Die Ausstellung und Prüfung der Berechtigung erfordert eine Verarbeitung personenbezogener Daten der Studierenden.

Die Parteien sind sich einig, dass die Verarbeitung personenbezogener Daten unter dem Hauptvertrag eine gemeinsame Verantwortlichkeit zwischen den Parteien im Sinne von Art. 26 DSGVO begründet. Die Einzelheiten der gemeinsamen Verarbeitung sind in den folgenden Bestimmungen („**Vereinbarung**") geregelt.

1. Gegenstand und Dauer der Vereinbarung

1.1 Diese Vereinbarung findet auf alle Tätigkeiten Anwendung, bei denen die Parteien unter dem Hauptvertrag personenbezogene Daten verarbeiten.

1.2 Für die Laufzeit und Beendigung des Vertrages gelten die Regelungen des Hauptvertrages.

1.3 Im Falle von Widersprüchen zwischen dieser Vereinbarung und dem Hauptvertrag gehen die Regelungen dieser Vereinbarung vor.

1.4 Soweit in dieser Vereinbarung nicht abweichend definiert, gelten die Definitionen des Hauptvertrags.

2. Bereiche und Art der gemeinsamen Verarbeitung

2.1 Die Parteien sind sich darüber einig, dass sie bei nachfolgend näher beschriebenen Verarbeitungstätigkeiten gemeinsam über Zwecke und Mittel der Verarbeitung bestimmen und insoweit eine gemeinsame Verantwortlichkeit für festgelegte Prozessabschnitte besteht:

2.1.1 <u>Datenbereitstellung</u>

Der Vertragspartner übermittelt an den Dienstleister per CSV-Datei die in **Anhang A** festgelegten Datenkategorien immatrikulierter Studierender, die zur Nutzung des Semestertickets berechtigt sind, insbesondere nicht befreit wurden (sogenannte White-List) oder stellt dem Dienstleister eine Schnittstelle zu der Software Shibboleth zur Verfügung, über die die Daten der Berechtigten abgerufen werden und die Berechtigungsprüfung stattfinden kann. Über Shibboleth werden nur die in **Anhang A** genannten Datenkategorien übermittelt.

2.1.2 <u>Mitteilungen an die Betroffenen</u>

Der Vertragspartner leitet den vom Dienstleister erstellten Link und/oder QR-Code zur App an Studierende weiter, um über den Aktivierungsprozess des DST zu informieren. Dies geschieht per E-Mail und/oder Brief.

2.1.3 Berechtigungsprüfung und Erstellung des DST

Der Dienstleister führt eine Berechtigungsprüfung durch, wenn der Betroffene in der App den Aktivierungsprozess startet und stellt bei einem Positivergebnis und nach Mitteilung weiterer erforderlicher Daten durch den Betroffenen (nach **Anhang A**) das DST aus.

2.2 Im Übrigen sind die Parteien im Hinblick auf alle nicht in dieser Vereinbarung geregelten Verarbeitungsprozesse eigenständige Verantwortliche im Sinne des Art. 4 Nr. 7 DSGVO.

2.3 Zweck, Mittel und Umfang der Verarbeitung personenbezogener Daten sowie die Art der verarbeiteten Daten und die Kategorien der betroffenen Personen sind im Hauptvertrag und der in **Anhang A** festgelegt.

2.4 Soweit dies wegen einer Änderung der Verarbeitungsvorgänge selbst und/oder aufgrund einer Änderung oder Ergänzung des Hauptvertrags erforderlich wird, werden die Parteien diese Vereinbarung und die Datenschutzinformationen für Betroffene entsprechend anpassen. Jede Partei wird die andere Partei darüber unterrichten, wenn sie eine Anpassung für erforderlich hält. Unbeschadet dessen wird jede der Parteien regelmäßig, zumindest aber einmal jährlich, prüfen, ob die in dieser Vereinbarung und ihren Anlagen geregelten Verarbeitungsvorgänge noch der tatsächlichen Handhabung entsprechen.

3. Aufgabenzuweisung

3.1 Die Parteien haben innerhalb der gemeinsamen Verantwortlichkeit eine Zuständigkeitsverteilung getroffen, die sich an den tatsächlichen Beiträgen und Einflussmöglichkeiten der Parteien orientiert, wie sie in Ziffer 2. dargestellt wird.

3.2 Die Parteien haben im Übrigen die gesetzlichen Aufgaben zusammenfassend untereinander wie folgt verteilt:

Pflichten aus der DSGVO	Vertragspartner	Verkehrsunternehmen	BBG	Erläuterungen und Verweise
Zweckfestlegung	X	X	X	Siehe Anhang A
Mittelfestlegung	X	X	X	Siehe Anhang A
Festlegung der Datenkategorien	X	X	X	Siehe Anhang A
Zur Verfügungstellung des Wesentlichen der Vereinbarung, Art. 26 Abs. 2 S. 2 DSGVO	X			Siehe Anhang B
Informationspflichten, Art. 13, 14 DSGVO	X	(X) Unterstützend	(X) Unterstützend	Siehe Anhang B

Bearbeitung von geltend gemachten Rechten, Art. 15 – 21 DSGVO	X	(X) Unterstützend	(X) Unterstützend	Siehe Ziffer 5
Festlegung der technischen und organisatorischen Maßnahmen, Art. 24 Abs. 1 i. V. m. Art. 32 DS-GVO	X	(X) Unterstützend	X	Siehe Ziffer 7 und Anhang C
Einschaltung von Auftragsverarbeitern und deren Überprüfung, Art. 28 DSGVO		(X)	X	Das Verkehrsunternehmen kontrolliert BBG in Bezug auf die Auftragsverarbeiter
Verarbeitungsverzeichnis, Art. 30 DSGVO	X	X	X	
Meldepflichten, Art. 33, 34 DSGVO	X		X	Siehe Ziffer 9, in Abhängigkeit der Zuständigkeiten
Datenschutz-Folgenabschätzung, Art. 35 DSGVO			X	Die Durchführung ist nach Prüfung der Verarbeitungstätigkeiten nicht notwendig.
Datenschutzbeauftragter, Art. 37 DSGVO	X	X	X	

3.3 Soweit Verantwortlichkeiten in dieser Vereinbarung nicht anderweitig geregelt sind, sind die Parteien gleichermaßen verantwortlich und werden sich in allen die Verarbeitung der Daten betreffenden Fragen austauschen.

3.4 Im Falle der Löschung von Daten sind die jeweils anderen Parteien vor der Löschung in Textform zu informieren. Ungeachtet der in 3.1 festgelegten Zuständigkeiten, kann jede Partei einer Löschung der Daten widersprechen, sofern sie eine gesetzliche Aufbewahrungspflicht trifft oder ihr ein berechtigtes Interesse an der weiteren Speicherung (z.B. zur Durchsetzung von Ansprüchen) zusteht.

3.5 Die Parteien dürfen die Daten nur innerhalb ihrer Zuständigkeiten und nur für die in **Anhang A** festgelegten Zwecke verarbeiten.

4. Rechtmäßigkeit der Datenverarbeitung

4.1 Die Parteien gewährleisten die Einhaltung der anwendbaren datenschutzrechtlichen Bestimmungen nach Maßgabe dieser Vereinbarung und für die dokumentierten Zwecke.

4.2 Ungeachtet der festgelegten Zuständigkeiten sind die Parteien gemeinsam für die Rechtmäßigkeit der Datenverarbeitung verantwortlich.

4.3 Rechtsgrundlage für die Erstellung der CSV-Datei mit den DST berechtigten Betroffenen und Übermittlung an den Dienstleister bzw. Freischaltung dieser Betroffenen bei

Shibboleth sowie die Mitteilung an den Betroffenen ist Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO bzw. für den Vertragspartner Art. 6 Abs. 1 UAbs. 1 lit. e DSGVO i.V.m. § 16 Abs. 1 Nr. 6 BbgHG, i.V.m. § 5 BbgDSG.

4.4 Die Rechtsgrundlage für die Datenverarbeitung zur Erstellung des DST ist die Vertragserfüllung bzw. vorvertragliche Maßnahmen auf Anfrage des Betroffenen nach Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO.

4.5 Sollte die Einholung von Einwilligungen für die Datenverarbeitung erforderlich sein, ist die Partei zuständig, die die Daten, für deren Verarbeitung die Einwilligung erforderlich ist, erhebt oder von der die Verarbeitung ausgeht. Einwilligungen haben den Anforderungen des Art. 7 und ggf. des Art. 9 DSGVO zu entsprechen. Insbesondere ist den Informationspflichten nachzukommen und die Betroffenen sind auf die Freiwilligkeit und das bestehende Widerrufsrecht hinzuweisen. Der Einwilligungsprozess ist in jedem Einzelfall zu dokumentieren.

4.6 Datenübermittlung in Drittländer, auch durch (Unter-) Auftragsverarbeiter, haben insbesondere den Art. 44 ff. DSGVO zu entsprechen.

5. Informationspflichten gegenüber den Betroffenen

5.1 Die Parteien haben die als **Anhang B** beigefügte Datenschutzinformation für Studierende abgestimmt. Die Parteien gehen davon aus, dass diese Information die Anforderungen nach Art. 12 bis 14 und 26 Abs. 2 S. 2 DSGVO erfüllen.

5.2 Der Vertragspartner verpflichtet sich, die Datenschutzinformation nach 5.1 rechtzeitig zur Verfügung zu stellen. Die Informationen werden rechtzeitig, mit Einholung einer Einwilligung der Betroffenen, mit Weiterleitung oder Veröffentlichung des Links zur App und/oder bei Eingabe der Daten in der App bereitgestellt.

5.3 Das Verkehrsunternehmen und BBG stellen dem Vertragspartner die zur Erfüllung der Pflicht erforderlichen Informationen zur Verfügung.

5.4 Als Ansprechpartner für Betroffene wird in der Datenschutzinformation der Vertragspartner mit entsprechenden Kontaktdaten angegeben („**Anlaufstelle**").

6. Erfüllung sonstiger Rechte der Betroffenen

6.1 Betroffene können die ihnen aus Art. 15 bis 22 DSGVO zustehenden Rechte gegenüber allen Parteien geltend machen.

6.2 Die Parteien sind sich einig, dass die Anlaufstelle der Auskunftspflicht nach Art. 15 DSGVO nachkommt und für die Erfüllung der sonstigen Betroffenenrechte zuständig ist. Bei dem Verkehrsunternehmen oder BBG eingehende Anfragen leiten diese unverzüglich an den Vertragspartner weiter.

6.3 Der Vertragspartner ist verpflichtet, die Beantwortung jedes Auskunftsersuchens und/oder die Gewährung der sonstigen Rechte mit dem Verkehrsunternehmen und BBG abzustimmen.

6.4 Soweit einer Partei die Umsetzung der geltend gemachten Betroffenenrechte nicht möglich ist, wird sie dies unverzüglich in Textform mitteilen. Die Parteien werden sich dann nach Treu und Glauben dazu abstimmen, wie die Betroffenenrechte in Übereinstimmung mit den gesetzlichen Regelungen sichergestellt werden können.

6.5 Die Kommunikation zwischen den Parteien im Rahmen der Erfüllung der Regelungen unter 6.1 und 6.2 erfolgt ausschließlich verschlüsselt über folgende E-Mail-Adressen:

Vertragspartner:	datenschutz@astaup.de
BBG:	datenschutz@bbg-eberswalde.de
Verkehrsunternehmen:	datenschutz@vip-potsdam.de

7. Sicherheit der Datenverarbeitung

7.1 Die Parteien implementieren und überwachen die in **Anhang C** spezifizierten technischen und organisatorischen Maßnahmen, die nach Maßgabe der Artikeln 32 und 25 DSGVO geeignet und erforderlich sind, ein dem Risiko für Rechte und Freiheiten der Betroffenen angemessenes Schutzniveau zu gewährleisten und die Datenschutzgrundsätze zu wahren.

7.2 Die Parteien sind hinsichtlich der Sicherheit der Datenverarbeitung wie folgt zuständig:

7.2.1 Der Vertragspartner ist zuständig für die Speicherung und Sicherung und Aktualität der Daten in ihren Systemen; (sofern relevant) die korrekte Einrichtung von Shibboleth; die regelmäßige Prüfung der Fehlerfreiheit und Sicherheit;

7.2.2 BBG ist zuständig, dass die übermittelten Daten gesichert, verfügbar und unverändert sind sowie für den Betrieb der App über den Dienstleister und der Implementierung und Einhaltung der technischen und organisatorischen Maßnahmen beim Betrieb der App;

7.2.3 Das Verkehrsunternehmen ist zuständig für die Sicherstellung regelmäßiger Kontrollen durch BBG beim Dienstleister, die Überprüfung der Kontrollergebnisse und die Angemessenheit der beim Dienstleister implementierten technischen und organisatorischen Maßnahmen.

7.3 Die in **Anhang C** spezifizierten Maßnahmen sind vor Beginn der Verarbeitung zu implementieren und müssen während der Dauer des Vertrages aufrechterhalten werden, sind sofern erforderlich dem technischen Stand anzupassen und dürfen das Schutzniveau in keinem Fall unterschreiten.

8. Auftragsverarbeiter

8.1 Die Beauftragung von Auftragsverarbeitern gemäß Art. 4 Nr. 8 DSGVO, soweit dies die gemeinsame Verantwortlichkeit betrifft, durch eine Partei bedarf der vorherigen schriftlichen Zustimmung der jeweils anderen Parteien und des Abschlusses eines Auftragsverarbeitungsvertrags nach Art. 28 DSGVO. Die Parteien stimmen bereits jetzt der Beauftragung der in **Anhang D** aufgeführten Auftragsverarbeiter zu.

8.2 Die Parteien informieren sich gegenseitig rechtzeitig in Textform vor jeder beabsichtigten Änderung in Bezug auf die Hinzuziehung oder Ersetzung von Auftragsverarbeitern und beauftragen nur solche Auftragsverarbeiter, die die Anforderungen des Datenschutzrechts und die Bestimmungen dieser Vereinbarung erfüllen.

8.3 Eine Verarbeitung von Daten durch Auftragsverarbeiter einer Partei in Drittstaaten bedarf, zusätzlich zu der vorherigen schriftlichen Zustimmung der Information in Textform über die Drittstaaten, in denen die Verarbeitung erfolgt, sowie über die betroffenen Daten und die Art und Umfang der Datenverarbeitung.

8.4 Auftragsverarbeiter sind von der beauftragenden Partei mindestens einmal jährlich in geeigneter Form zu prüfen. Der dabei erstellte Prüfbericht ist den anderen Parteien auf Verlangen zur Verfügung zu stellen.

8.5 Jede Partei steht für Handlungen ihrer Auftragsverarbeiter wie für eigene Handlungen ein.

9. Vorgehen bei Datenschutzverletzungen und Anfragen von Aufsichtsbehörden

9.1 Für die Prüfung und Bearbeitung aller Verletzungen des Schutzes personenbezogener Daten, die aus der Sphäre des Vertragspartners stammen, insbesondere in die Zuständigkeit nach 2.1.1 und 2.1.2, einschließlich der Erfüllung deshalb bestehender Meldepflichten gegenüber der zuständigen Aufsichtsbehörde nach Art. 33 DSGVO und den Betroffenen nach Art. 34 DSGVO ist der Vertragspartner zuständig. In den übrigen Fällen BBG.

9.2 Wird einer der Parteien eine Verletzung des Datenschutzes bekannt oder tritt eine sicherheitsrelevante Störung des Datenverarbeitungsprozesses auf, sind die Parteien ungeachtet der Zuständigkeitsverteilung nach 9.1 verpflichtet, innerhalb ihrer Organisation unverzüglich Maßnahmen zu ergreifen, die zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen erforderlich sind. Der Vorfall ist den jeweils anderen Parteien unverzüglich in Textform zu melden.

9.3 Jede Partei zeigt den jeweils anderen Parteien unverzüglich in Textform an, wenn sich eine Aufsichtsbehörde im Zusammenhang mit der Verarbeitung von Daten unter diesem Vertrag an sie wendet. Die Parteien werden den Aufforderungen zuständiger Aufsichtsbehörden Folge leisten, insbesondere in Bezug auf Anfragen und die Überlassung von Informationen.

9.4 Vor einer Meldung nach 9.1 oder Beantwortung einer Anfrage einer Aufsichtsbehörde nach 9.3 stimmen sich die Parteien hinsichtlich des Vorgehens ab und unterstützen sich gegenseitig soweit rechtlich und tatsächlich möglich. Eine Abstimmung ist nicht notwendig, wenn die Abstimmung mit erheblichen rechtlichen oder tatsächlichen Schwierigkeiten verbunden ist. Die Pflicht zur Anzeige in Textform nach 9.3 ist hiervon nicht betroffen.

10. Sonstige Pflichten der Parteien

10.1 Jede Partei hat die anderen Parteien unverzüglich und vollständig in Textform zu informieren, wenn sie einen Fehler oder Unregelmäßigkeiten bei der Datenverarbeitung oder der Verletzungen von Bestimmungen dieses Vertrags oder anwendbaren Datenschutzrechts feststellt oder vermutet.

10.2 Dokumentationen im Sinne von Art. 5 Abs. 2 DSGVO, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, werden durch jede Partei entsprechend den rechtlichen Befugnissen und Verpflichtungen über das Vertragsende hinaus aufbewahrt.

11. Haftung

11.1 Unbeschadet der Regelungen dieser Vereinbarung und des Hauptvertrages haften die Parteien für den Schaden, der durch eine nicht den datenschutzrechtlichen Bestimmungen entsprechende Verarbeitung von Daten verursacht wird, im Außenverhältnis als Gesamtschuldner gegenüber den betroffenen Personen (Art. 82 DSGVO).

11.2 Im Innenverhältnis haften die Parteien einander nur für ihren Anteil an der haftungsauslösenden Ursache:

11.2.1 Macht ein Betroffener einen Anspruch gegenüber einer Partei geltend, der nicht dem Verantwortungsanteil an dem Verstoß entspricht, sind die jeweils anderen Parteien verpflichtet, die in Anspruch genommene Partei in dem Umfang freizustellen, in dem sie die Verantwortung für den sanktionierten Verstoß tragen.

11.2.2 Im Fall der Verhängung von Geldbußen gilt Folgendes: Die mit der Geldbuße belegte Partei muss die Rechtsmittel gegen den Bußgeldbescheid ausgeschöpft haben. Bleibt die Partei danach ganz oder teilweise mit einer Geldbuße belastet, die nicht ihrem internen Anteil an der Verantwortung für den Verstoß entspricht, sind die jeweils anderen Parteien verpflichtet, sie in dem Umfang von der Geldbuße freizustellen, in dem sie jeweils die Verantwortung für den Verstoß haben.

12. Schlussbestimmungen

12.1 Mündliche Nebenabreden bestehen nicht. Änderungen oder Ergänzungen dieses Vertrages einschließlich dieser Bestimmung bedürfen zu ihrer Wirksamkeit der Schriftform. Dies gilt auch für die Änderung dieses Schriftformerfordernisses.

12.2 Sollte eine Bestimmung dieses Vertrages ganz oder teilweise nichtig, unwirksam oder nicht durchsetzbar sein oder werden, oder sollte eine an sich notwendige Regelung nicht enthalten sein, werden die Wirksamkeit und die Durchsetzbarkeit aller übrigen Bestimmungen dieses Vertrages nicht berührt. Anstelle der nichtigen, unwirksamen oder nicht durchsetzbaren Bestimmung oder zur Ausfüllung der Regelungslücke werden die Parteien eine rechtlich zulässige Regelung vereinbaren, die so weit wie möglich dem entspricht, was die Parteien gewollt haben oder nach dem Sinn und Zweck dieses Vertrages vereinbart haben würden, wenn sie die Unwirksamkeit oder die Regelungslücke erkannt hätten. Es ist der ausdrückliche Wille der Parteien, dass diese salvatorische Klausel keine bloße Beweislastumkehr zur Folge hat, sondern § 139 BGB insgesamt abbedungen ist.

Unterschriften auf der folgenden Seite

Unterschriften

Vertragspartner

Datum:	20.03.24	Datum:	20.03.2024
Name:	Sophie Schreyer	Name:	~~Simon Berner~~
Position:	Vorstand AStA	Position:	Vorstand AStA

BBG

Datum:		Datum:	
Name:	Frank Wruck	Name:	
Position:	Geschäftsführer	Position:	

Verkehrsunternehmen

Datum:		Datum:	
Name:	Uwe Loeschmann	Name:	Bettina Biffi
Position:	Geschäftsführer	Position:	Geschäftsführerin

Anhang A

Beschreibung der Datenverarbeitung

Datenkategorien

Nutzung der CSV-Datei:

- Vorname und Nachname
- Hochschulspezifische Daten (Matrikelnummer, besuchte Hochschule, ID)
- Gültigkeitszeitraum
- Geburtsdatum

Nutzung von Shibboleth:

- Vorname und Nachname
- Status zur Semesterticketberechtigung und Gültigkeitszeitraum
- Hochschulspezifische Daten (besuchte Hochschule, ID, optional Matrikelnummer)
- Geburtsdatum

Kategorien der Betroffenen:

- Studierende

Zwecke der Datenverarbeitung:

Der gemeinsam festgelegte Zweck der Datenverarbeitung ist die Bereitstellung des DST im Sinne eines Digitaltickets für die Studierenden. sowie die Erbringung von Supportleistungen durch den Dienstleister.

Mittel der Datenverarbeitung:

Zur Erreichung der Zwecke legen die Parteien die Mittel der Datenverarbeitung, mithin die Art und Weise der Verarbeitung und technische und organisatorische Gegebenheiten bei der Verarbeitung wie folgt fest:

Der Datenabgleich zur Berechtigungsprüfung zum Erhalt des DST findet entweder

(1) mittels einer CSV-Datei statt, die die oben genannten Datenkategorien enthält, welche über einen SFTP-Server an den Dienstleister übermittelt werden, oder

(2) über die Schnittstelle der Software Shibboleth, welche von Hochschulen zur Authentifizierung und Autorisierung der Studierenden für Webservices und Webanwendungen genutzt wird.

Der Aktivierungsprozess wird über die App des Dienstleisters umgesetzt.

Anhang B

Datenschutzinformation für Studierende

Deutschlandsemesterticket

Liebe Studierende,

von der Einführung des bundesweit gültigen Deutschlandtickets zum 1. Mai 2023 sollen auch Sie, als Studierende profitieren. Ihr Semesterbeitrag beinhaltet grundsätzlich bereits die Kosten für ein vergünstigtes Deutschlandticket (nachfolgend „**Deutschlandsemesterticket**"). Das Deutschlandsemesterticket wird als rein digitales Ticket angeboten. Sie können Ihr persönliches Deutschlandsemesterticket über die Web-Applikation RIDEcampus des Dienstleisters Digital H GmbH („**App-Betreiber**") aktivieren.

Die Bereitstellung dieses Angebots ist mit der Verarbeitung Ihrer personenbezogenen Daten verbunden. Wir möchten Ihnen daher die folgenden Informationen bereitstellen.

1. Verantwortlicher und Anlaufstelle

Bei Fragen rund um die Datenverarbeitung und die Geltendmachung von Rechten (siehe dazu Ziffer 9) können Sie sich gerne an folgenden Verantwortlichen wenden, der zugleich die sogenannte Anlaufstelle ist:

Studierendenschaft der Universität Potsdam Am Neuen Palais 10, 14469 Potsdam E-Mail: vorstand@astaup.de („**Studierendenschaft**") Kontakt Datenschutzbeauftragte: Datenschutzbeauftragte der Studierendenschaft der Universität Potsdam Am Neuen Palais 10, 14469 Potsdam E-Mail: datenschutz@astaup.de

2. Weitere Verantwortliche und Datenschutzbeauftragte

Es besteht eine gemeinsame Verantwortlichkeit mit dem Verkehrsunternehmen, mit dem die Studierendenschaft einen Vertrag über das Deutschlandsemesterticket geschlossen hat:

ViP Verkehrsbetrieb Potsdam GmbH
Fritz-Zubeil-Straße 96, 14482 Potsdam

Datenschutzbeauftragter:

Dr. Martin Schmidt
E-Mail: datenschutz@vip-potsdam.de

(„**vertragshaltendes Verkehrsunternehmen**")

und einem weiteren Verkehrsunternehmen:

Barnimer Busgesellschaft mbH
Poratzstraße 68, 16225 Eberswalde

Datenschutzbeauftragter:

Hardy Brüggemann
E-Mail: datenschutz@bbg-eberswalde.de

(„**BBG**").

Diese Verantwortlichen haben eine Vereinbarung über die gemeinsame Verantwortlichkeit geschlossen und sich darauf verständigt, dass die Studierendenschaft als Anlaufstelle fungiert und Sie über die Datenverarbeitung im Zusammenhang mit dem Deutschlandsemesterticket informiert. Wenn Sie Rechte nach Ziffer 9 geltend machen, werden diese primär von der Studierendenschaft, ggf. mit Unterstützung der weiteren Verantwortlichen bearbeitet.

3. Zweck und Rechtsgrundlagen der Datenverarbeitung

Bei der Verarbeitung von personenbezogenen Daten, die für die Vertragserfüllung erforderlich sind, ist Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO die Rechtsgrundlage. Dies gilt auch für Verarbeitungsvorgänge, die bereits vorvertraglich relevant werden. Auf dieser Rechtsgrundlage findet die Datenverarbeitung während des Aktivierungsprozesses in der Web-App statt, der eine Berechtigungsprüfung und Ausstellung sowie Versendung der Deutschlandsemestertickets umfasst.

Ist die Verarbeitung zur Wahrung unseres berechtigten Interesses erforderlich und überwiegen Ihre Interessen, Grundrechte und Grundfreiheiten nicht unsere Interessen, so dient Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO als Rechtsgrundlage für die Verarbeitung; für die Studierendenschaft wird die Verarbeitung auf Art. 6 Abs. 1 UAbs. 1 lit. e DSGVO i.V.m. § 16 Abs. 1 Nr. 6 BbgHG, i.V.m. § 5 BbgDSG (Ausübung öffentlicher Gewalt im

Sinne der Ausübung hoheitlicher Befugnisse) gestützt. Wir haben ein berechtigtes Interesse, Ihnen Informationen zum Deutschlandsemesterticket und zum Aktivierungsprozess über den App-Betreiber zuzusenden. Außerdem stellen wir auf dieser Rechtsgrundlage dem App-Betreiber die erforderlichen Daten zur Verfügung, um eine Berechtigungsprüfung im Rahmen des von Ihnen angestoßenen Aktivierungsprozesses durchführen zu können. Als Studierendenschaft haben wir die Aufgabe, die Interessen der Studierenden z.B. auch die sozialen Belange wahrzunehmen (vgl. § 16 BbgHG), dazu gehören auch Tätigkeiten, die zur Ermöglichung eines preisgünstigen ÖPNV und SPNV Tickets für die Studierenden erforderlich sind.

4. Kategorien personenbezogener Daten

Wir verarbeiten nur solche personenbezogenen Daten, die für die genannten Zwecke erforderlich sind. Dabei wird es sich um folgende Datenkategorien handeln:

- Vorname und Nachname
- Status zur Semesterticketberechtigung und Gültigkeitszeitraum
- Hochschulspezifische Daten (besuchte Hochschule, ID, Matrikelnummer)
- Geburtsdatum

Wir möchten Sie darauf hinweisen, dass das Verkehrsunternehmen und BBG zwar auch Verantwortliche sind, die oben genannten Datenkategorien jedoch im Rahmen des regulären Aktivierungsprozesses nicht erhalten. Ihre Studierendenschaft bzw. die Hochschule stellt die Daten direkt dem App-Betreiber zur Verfügung. Der App-Betreiber greift auf die Daten nur dann zu, wenn Sie über die App den Aktivierungsprozess starten und die Berechtigungsprüfung stattfindet.

5. Bereitstellung von Daten

Zur Bereitstellung von Daten sind Sie nicht verpflichtet. Wir weisen Sie jedoch darauf hin, dass wir ohne die Bereitstellung der erforderlichen Daten im Aktivierungsprozess nicht in der Lage sind, Ihnen das Deutschlandsemesterticket auszustellen.

6. Empfänger personenbezogener Daten

Ihre Daten werden nur für die festgelegten Zwecke und den dafür zuständigen Abteilungen und Personen verarbeitet.

Eine Datenweitergabe erfolgt an den App-Betreiber, der die digitalen Deutschlandsemestertickets erstellt und an Sie versendet. Bei dem Dienstleister handelt es sich um die: Digital H GmbH, Am Bahndamm 2, 41516 Grevenbroich. Mit dem App-Betreiber wurde ein Auftragsverarbeitungsvertrag geschlossen. Weitere Informationen zur Datenverarbeitung über die App finden Sie unter: https://ride-ticketing.de/datenschutzerklarung.

7. Datenverarbeitung in Drittländern

Wir verarbeiten Ihre personenbezogenen Daten nur im Europäischen Wirtschaftsraum. Sofern eine Übermittlung in ein Drittland stattfindet, erfolgt dies nur vorbehaltlich der in Art. 44 ff. DSGVO niedergelegten Bedingungen.

8. Datenspeicherung, Aufbewahrung und Löschung

Ihre personenbezogenen Daten werden nur so lange verarbeitet und gespeichert, wie dies zur Erfüllung der vertraglichen und gesetzlichen Zwecke erforderlich ist. Die an den App-Betreiber übermittelten Daten werden für den von uns festgelegten Gültigkeitszeitraum gespeichert. Der Gültigkeitszeitraum beträgt stets ein Semester.

Nach Ablauf der jeweiligen Aufbewahrungsfrist werden Ihre Daten gelöscht. Eine darüber hinausgehende Speicherdauer kommt in Betracht, wenn die personenbezogenen Daten zur Verteidigung oder Ausübung von Rechtsansprüchen erforderlich sind oder Ihre Einwilligung vorliegt.

Stellt die Studierendenschaft dem App-Betreiber aktualisierte Daten zur Berechtigungsprüfung bereit, löscht der App-Betreiber die alte Fassung nach 6 Monaten. Der App-Betreiber löscht spätestens mit Beendigung seines Auftrags vorhandene personenbezogene Daten.

9. Ihre Rechte

9.1 Sie können jederzeit im Rahmen der gesetzlichen Bestimmungen Auskunft über Ihre von uns verarbeiteten personenbezogenen Daten verlangen (Art. 15 DSGVO).

9.2 Sie haben ein Recht auf Berichtigung und/oder Vervollständigung Ihrer Daten, sofern die Sie betreffenden verarbeiteten personenbezogenen Daten unrichtig oder unvollständig sind (Art. 16 DSGVO).

9.3 Sie können von uns verlangen, dass die Sie betreffenden personenbezogenen Daten unverzüglich gelöscht werden, sofern die Voraussetzungen hierfür vorliegen. Das Recht auf Löschung besteht nicht, soweit die Verarbeitung erforderlich ist (Art. 17 DSGVO).

9.4 Liegen die Voraussetzungen hierfür vor, können Sie die Einschränkung der Verarbeitung Ihrer personenbezogenen Daten verlangen (Art. 18 DSGVO).

9.5 Haben Sie das Recht auf Berichtigung, Löschung oder Einschränkung der Verarbeitung gegenüber uns geltend gemacht, sind wir verpflichtet, allen Empfängern, denen die Sie betreffenden personenbezogenen Daten offengelegt wurden, diese Berichtigung oder Löschung der Daten oder Einschränkung der Verarbeitung mitzuteilen, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden. Wir unterrichten Sie über diese Empfänger auf Verlangen (Art. 19 DSGVO).

9.6 Sie haben das Recht, die Sie betreffenden personenbezogenen Daten, die Sie bereitgestellt haben, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten. Außerdem haben Sie das Recht, diese Daten einem anderen Unternehmen zu übermitteln, sofern die Voraussetzungen hierfür vorliegen (Art. 20 DSGVO).

9.7 **Widerspruchsrecht**

Sie haben das Recht, aus Gründen, die sich aus Ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung der Sie betreffenden personenbezogenen Daten, die aufgrund von Art. 6 Abs. 1 UAbs. 1 lit. e, f DSGVO erfolgt, Widerspruch einzulegen (Art. 21 Abs. 1 DSGVO). Folge des Widerspruchs ist es, dass wir die Sie betreffenden personenbezogenen Daten nicht mehr verarbeiten, es sei denn, wir können zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die Ihre Interessen, Rechte und Freiheiten überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

9.8 Sofern Sie eine datenschutzrechtliche Einwilligungserklärung abgegeben haben, können Sie diese jederzeit widerrufen (Art. 7 DSGVO). Der Widerruf der Einwilligung wirkt erst für die Zukunft. Daher wird die Rechtmäßigkeit, der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung, nicht berührt.

9.9 Unbeschadet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs steht Ihnen das Recht auf Beschwerde bei einer Aufsichtsbehörde, insbesondere in dem Mitgliedstaat ihres Aufenthaltsorts, ihres Arbeitsplatzes oder des Ortes des mutmaßlichen Verstoßes, zu, wenn Sie der Ansicht sind, dass die Verarbeitung der Sie betreffenden personenbezogenen Daten gegen die DSGVO verstößt (Art. 77 DSGVO).

Anhang C

Technische und organisatorische Maßnahmen

Die Parteien treffen die folgenden technischen und organisatorischen Maßnahmen:

I. Vertragspartner

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

Die Verarbeitung personenbezogener Daten erfolgt in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen (Bsp.: Ersetzung eines Klarnamens durch eine User-ID).

2. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

2.1 Zutrittskontrolle: Schließ- und Sicherheitssystem verhindern den unbefugten Zutritt zu den Datenverarbeitungsanlagen.

2.2 Zugangskontrolle: Der unbefugte Zugang zu den Datenverarbeitungssystemen wird durch folgende Maßnahmen verhindert:

- Authentifikation mit Benutzer und Passwort
- Zentrale Passwortregeln (Passwort-Richtlinie)
- Automatische Sperrmechanismen (z.B. Desktopsperre nach 10 Minuten Inaktivität)
- Zwei-Faktor-Authentifizierung
- Verschlüsselung von Datenträgern

2.3 Zugriffskontrolle: Der Zugriff auf personenbezogene Daten durch Unbefugte wird durch folgende Maßnahmen verhindert:

- Anzahl der Administratoren wird möglichst gering gehalten
- Benutzerrechte werden durch Systemadministratoren verwaltet und bedarfsabhängig vergeben
- Protokollierung von Zugriffen (insb. bei der Eingabe, Löschung und Änderungen von Daten)

2.4 Trennungskontrolle: Zu unterschiedlichen Zwecken erhobene personenbezogene Daten werden getrennt verarbeitet. Dies wird durch folgende Maßnahmen gewährleistet:

- Mandantenfähigkeit
- Physisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- Speicherung von personenbezogenen Daten in Abhängigkeit des jeweiligen Zwecks in unterschiedlichen Datenbanken/Bereichen
- Trennung von Produktiv- und Testsystemen

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

3.1 Weitergabekontrolle: Es wird sichergestellt, dass personenbezogene Daten bei der Übertragung oder Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden:

- Verschlüsselung
- Elektronische Signatur
- Datenbereitstellung über verschlüsselte Verbindungen

3.2 Eingabekontrolle: Es wird sichergestellt, dass eine Prüfung stattfinden kann, wann und wer welche personenbezogenen Daten verarbeitet hat, durch:

- Protokollierung der Eingabe, Änderung, Löschung von Daten
- Kontrolle der Protokolle
- Nachvollziehbarkeit der Verarbeitung durch individuelle Benutzerkennung
- Dokumentenmanagement
- Ggf. Bestätigung der Richtigkeit der gespeicherten Daten durch den Betroffenen

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

Die nachfolgenden Maßnahmen stellen sicher, dass personenbezogene Daten gegen zufällige oder mutwillige Zerstörung oder Verlust geschützt sind und verfügbar sind:

- Backup-Strategie (online/offline; on-site/off-site), insb. regelmäßiges Backup, Aufbewahrung von Datensicherung an einem sicheren und ausgelagerten Ort
- Virenschutz
- Firewall
- Meldewege und Notfallpläne
- Feuer- und Rauchmelder, Löschanlagen
- Regelmäßige System- und Softwareupdates

5. Verfahren zur Wiederherstellung der Verfügbarkeit (Art. 32 Abs. 1 lit. c DSGVO)

- Regelmäßige Tests der Funktionsfähigkeit des Datenwiederherstellungssystems
- Notfallkontakt IT

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

6.1 Datenschutz-Management

- Datenschutzkonzept
- Interne Verhaltensregeln
- Verpflichtung auf das Datengeheimnis und auf die Vertraulichkeit sowie Ablage der unterschriebenen Erklärungen
- Protokolle Datensicherheit

- Rollenkonzepte (Bsp. Vertreterregelungen für IT-Leiter bei Krankheit/Abwesenheit)
- Bestellung eines Datenschutzbeauftragten
- Regelmäßige Schulung der Mitarbeiter im Datenschutz (externe/interne Seminare, Online-Kurse, quartalsweise Informations-E-Mails zur „Auffrischung") und individuelle Schulung neuer Mitarbeiter
- Erstellung und Pflege eines Verzeichnisses der Verarbeitungstätigkeiten nach Art. 30 DSGVO
- Überprüfung der Umsetzung der Maßnahmen und Aktualität der Unterlagen
- Durchführung von Datenschutz-Folgenabschätzungen nach Art. 35 DSGVO bzw. Schwellenanalysen sowie Dokumentation der Ergebnisse

6.2 Incident-Response-Management

- Klare Dokumentation und Zuständigkeitsverteilung der Meldeprozesse für Datenschutzverletzungen nach Art. 4 Nr. 12 DSGVO gegenüber Aufsichtsbehörden (Art. 33 DSGVO) und Betroffenen (Art. 34 DSGVO).
- Einbindung des Datenschutzbeauftragten in Sicherheitsvorfälle und Datenpannen.

6.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO) werden durch „Privacy by design" und „Privacy by default" erreicht. Es werden nicht mehr Daten erhoben als für den jeweiligen Zweck erforderlich.

7. Auftragskontrolle

Personenbezogene Daten werden nur entsprechend der Weisung des Verantwortlichen verarbeitet. Dies wird sichergestellt durch:

- Eindeutige Vertragsgestaltung
- formalisiertes Auftragsmanagement (schriftliche Weisungen)
- strenge Auswahl des Dienstleisters
- Vorabüberzeugungspflicht
- Nachkontrollen (Sicherstellung der Löschung, Vernichtung durch Einholung von schriftlichen Bestätigungen)
- Einholung schriftlicher Bestätigungen, dass Mitarbeiter des Auftragsverarbeiters ebenfalls auf das Datengeheimnis verpflichtet sind

II. BBG

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

1.1 Zugangskontrolle: Der unbefugte Zugang zu den Datenverarbeitungssystemen wird durch folgende Maßnahmen verhindert:

- Authentifikation mit Benutzer und Passwort
- Zentrale Passwortregeln (Passwort-Richtlinie)
- Automatische Sperrmechanismen (z.B. Desktopsperre nach 10 Minuten Inaktivität)

- Zwei-Faktor-Authentifizierung
- Verschlüsselung von Datenträgern

1.2 Zugriffskontrolle: Der Zugriff auf personenbezogene Daten durch Unbefugte wird durch folgende Maßnahmen verhindert:

- Anzahl der Administratoren wird möglichst gering gehalten
- Benutzerrechte werden durch Systemadministratoren verwaltet und bedarfsabhängig vergeben
  Protokollierung von Zugriffen (insb. bei der Eingabe, Löschung und Änderungen von Daten)

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

2.1 Weitergabekontrolle: Es wird sichergestellt, dass personenbezogene Daten bei der Übertragung oder Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden:

- Verschlüsselung
- Elektronische Signatur
- Datenbereitstellung über verschlüsselte Verbindungen

2.2 Eingabekontrolle: Es wird sichergestellt, dass eine Prüfung stattfinden kann, wann und wer welche personenbezogenen Daten verarbeitet hat, durch:

- Protokollierung der Eingabe, Änderung, Löschung von Daten
- Kontrolle der Protokolle
- Nachvollziehbarkeit der Verarbeitung durch individuelle Benutzerkennung
- Dokumentenmanagement
- Ggf. Bestätigung der Richtigkeit der gespeicherten Daten durch den Betroffenen

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

Die nachfolgenden Maßnahmen stellen sicher, dass personenbezogene Daten gegen zufällige oder mutwillige Zerstörung oder Verlust geschützt sind und verfügbar sind:

- Backup-Strategie (online/offline; on-site/off-site), insb. regelmäßiges Backup, Aufbewahrung von Datensicherung an einem sicheren und ausgelagerten Ort
- Virenschutz
- Firewall

4. Verfahren zur Wiederherstellung der Verfügbarkeit (Art. 32 Abs. 1 lit. c DSGVO)

- Regelmäßige Tests der Funktionsfähigkeit des Datenwiederherstellungssystems

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

5.1 Datenschutz-Management

- Datenschutzkonzept

- Interne Verhaltensregeln
- Verpflichtung auf das Datengeheimnis und auf die Vertraulichkeit sowie Ablage der unterschriebenen Erklärungen
- Protokolle Datensicherheit
- Rollenkonzepte (Bsp. Vertreterregelungen für IT-Leiter bei Krankheit/Abwesenheit)
- Bestellung eines Datenschutzbeauftragten
- Regelmäßige Schulung der Mitarbeiter im Datenschutz (externe/interne Seminare, Online-Kurse, quartalsweise Informations-E-Mails zur „Auffrischung") und individuelle Schulung neuer Mitarbeiter
- Erstellung und Pflege eines Verzeichnisses der Verarbeitungstätigkeiten nach Art. 30 DSGVO
- Überprüfung der Umsetzung der Maßnahmen und Aktualität der Unterlagen
- Durchführung von Datenschutz-Folgenabschätzungen nach Art. 35 DSGVO bzw. Schwellenanalysen sowie Dokumentation der Ergebnisse

5.2 Incident-Response-Management

- Klare Dokumentation und Zuständigkeitsverteilung der Meldeprozesse für Datenschutzverletzungen nach Art. 4 Nr. 12 DSGVO gegenüber Aufsichtsbehörden (Art. 33 DSGVO) und Betroffenen (Art. 34 DSGVO).
- Einbindung des Datenschutzbeauftragten in Sicherheitsvorfälle und Datenpannen.

5.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO) werden durch „Privacy by design" und „Privacy by default" erreicht. Es werden nicht mehr Daten erhoben als für den jeweiligen Zweck erforderlich.

6. Auftragskontrolle

Personenbezogene Daten werden nur entsprechend der Weisung des Verantwortlichen verarbeitet. Dies wird sichergestellt durch:

- Eindeutige Vertragsgestaltung
- formalisiertes Auftragsmanagement (schriftliche Weisungen)
- strenge Auswahl des Dienstleisters
- Vorabüberzeugungspflicht
- Nachkontrollen (Sicherstellung der Löschung, Vernichtung durch Einholung von schriftlichen Bestätigungen)
- Einholung schriftlicher Bestätigungen, dass Mitarbeiter des Auftragsverarbeiters ebenfalls auf das Datengeheimnis verpflichtet sind

7. Technische und organisatorische Maßnahme der beauftragten Auftragsverarbeiters

- TOM Digital H GmbH

- Backup-Strategie (online/offline; on-site/off-
  Aufbewahrung von Datensicherung an eine
- Virenschutz
- Firewall

3. Verfahren zur regelmäßigen Überprüfung, Bew
Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

3.1 Datenschutz-Management

- Datenschutzkonzept
- Interne Verhaltensregeln
- Verpflichtung auf das Datengeheimnis und
  der unterschriebenen Erklärungen
- Rollenkonzepte (Bsp. Vertreterregelungen f
  heit)
- Bestellung eines Datenschutzbeauftragten
- Regelmäßige Schulung der Mitarbeiter im D
  nare, Online-Kurse, quartalsweise Informati
  individuelle Schulung neuer Mitarbeiter
- Erstellung und Pflege eines Verzeichnisses
  Art. 30 DSGVO
- Überprüfung der Umsetzung der Maßnahm

Datenverarbeitungssystemen wird

ie)

sktopsperre nach 10 Minuten Inakti-

e Daten durch Unbefugte wird durch

gering gehalten

istratoren verwaltet und bedarfsab-

Eingabe, Löschung und Änderungen

lit. b DSGVO)

ss personenbezogene Daten gegen
eschützt sind und verfügbar sind:
-site), insb. regelmäßiges Backup,
m sicheren und ausgelagerten Ort

III. Verkehrsunternehmen

vertung und Evaluierung (Art. 32

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

1.1 Zugangskontrolle: Der unbefugte Zugang zu den
durch folgende Maßnahmen verhindert:

- Authentifikation mit Benutzer und Passwort
- Zentrale Passwortregeln (Passwort-Richtlin
- Automatische Sperrmechanismen (z.B. Des
  vität)
- Zwei-Faktor-Authentifizierung

auf die Vertraulichkeit sowie Ablage

ür IT-Leiter bei Krankheit/Abwesen-

1.2 Zugriffskontrolle: Der Zugriff auf personenbezogene
folgende Maßnahmen verhindert:

- Anzahl der Administratoren wird möglichst
- Benutzerrechte werden durch Systemadmin
  hängig vergeben
- Protokollierung von Zugriffen (insb. bei der E
  von Daten)

Datenschutz (externe/interne Semi-
ons-E-Mails zur „Auffrischung") und

s der Verarbeitungstätigkeiten nach

en und Aktualität der Unterlagen

2. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1

Die nachfolgenden Maßnahmen stellen sicher, das

3.2 Incident-Response-Management

- Klare Dokumentation und Zuständigkeitsverteilung der Meldeprozesse für Datenschutzverletzungen nach Art. 4 Nr. 12 DSGVO gegenüber Aufsichtsbehörden (Art. 33 DSGVO) und Betroffenen (Art. 34 DSGVO).
- Einbindung des Datenschutzbeauftragten in Sicherheitsvorfälle und Datenpannen.

3.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO) werden durch „Privacy by design" und „Privacy by default" erreicht. Es werden nicht mehr Daten erhoben als für den jeweiligen Zweck erforderlich.

4. Auftragskontrolle

Personenbezogene Daten werden nur entsprechend der Weisung des Verantwortlichen verarbeitet. Dies wird sichergestellt durch:

- Eindeutige Vertragsgestaltung
- formalisiertes Auftragsmanagement (schriftliche Weisungen)
- strenge Auswahl des Dienstleisters
- Vorabüberzeugungspflicht
- Nachkontrollen (Sicherstellung der Löschung, Vernichtung durch Einholung von schriftlichen Bestätigungen)
- Einholung schriftlicher Bestätigungen, dass Mitarbeiter des Auftragsverarbeiters ebenfalls auf das Datengeheimnis verpflichtet sind

Anlage D

Auftragsverarbeiter

Der Vertragspartner hat Auftragsverarbeitungsverträge mit folgenden Personen geschlossen:

Auftragsverarbeiter	**Beschreibung**
Universität Potsdam Am Neuen Palais 10 14469 Potsdam	Übermittlung der zur Ausstellung des Deutschlandsemestertickets erforderlichen Daten via CSV-Datei an den Dienstleister Digital H.

BBG hat Auftragsverarbeitungsverträge mit folgenden Personen geschlossen:

Auftragsverarbeiter	**Beschreibung**
Digital H GmbH Am Bahndamm 2 41516 Grevenbroich („**Dienstleister**“)	Der Dienstleister wird als Auftragsverarbeiter eingesetzt, nimmt im Auftrag von BBG, und nach Anfrage des Betroffenen (im Sinne des Beginns des Aktivierungsprozesses), die Berechtigungsprüfung der Studierenden vor, auf Grundlage der vom Vertragspartner übermittelten und den Studierenden angegebenen Daten. Der Dienstleister übernimmt das Hosting der App und den 2nd und 3rd Level Support.