GEORG-AUGUST-UNIVERSITÄT
GÖTTINGEN

Vereinbarung
zur IT-Rahmendienstvereinbarung
zur Einführung, Anwendung und wesentlichen Änderung
der Zutrittssysteme

zwischen

der Georg-August-Universität Göttingen/
Georg-August-Universität Göttingen
Stiftung Öffentlichen Rechts
(Stiftungsuniversität)
- vertreten durch den Präsidenten -

und

dem Personalrat der Georg-August-Universität Göttingen
(ohne Universitätsmedizin Göttingen)
- vertreten durch den Vorsitzenden -

In Ergänzung zur IT-Rahmendienstvereinbarung (§ 2 Abs. 3 S. 3 IT-RDV) in der Fassung vom 19.09.2018 (veröffentlicht in den Amtlichen Mitteilungen I Nr. 53 vom 05.10.2018, S. 1216 ff.) wird zwischen dem Präsidium der Georg-August-Universität Göttingen/Georg-August-Universität Göttingen Stiftung Öffentlichen Rechts und dem Personalrat der Georg-August-Universität Göttingen (ohne Universitätsmedizin Göttingen) die Vereinbarung zur Einführung, Anwendung und wesentlichen Änderung der **Zutrittssysteme** abgeschlossen und ersetzt die seit dem 27.03.2003 gültige Dienstvereinbarung Zutrittssystem.

Diese Vereinbarung beinhaltet die systemspezifischen Bestimmungen zum Betrieb des o. g. IT-Systems. Sie dient zudem der allgemeinverständlichen Information gegenüber den Nutzern und wird in den Amtlichen Mitteilungen I veröffentlicht.

Die Systemdokumentationen (Anhänge 2.1 bis 2h), die Bestandteil der Vereinbarung sind, beinhalten detaillierte Bestimmungen zum Betrieb der o. g. IT-Systeme und werden nicht veröffentlicht.

Anlagen:

Anlage 1	Systemformular für die Zutrittssysteme
Anlage 2.1	Systemdokumentation Zutrittssystem AEOS
Anlage 2.2	Systemdokumentation Zutrittssystem SiPort
Anlage 2a	Berechtigungskonzept
Anlage 2b.1	Betriebskonzept Zutrittssystem AEOS
Anlage 2b.2	Betriebskonzept Zutrittssystem SiPort
Anlage 2c	Leistungsbeschreibung Zutrittssystem AEOS
Anlage 2d.1	Sicherheitskonzept Zutrittssystem AEOS
Anlage 2d.2	Verfahrensanweisung Zutrittssystem SiPort
Anlage 2e	Verarbeitungstätigkeitsbeschreibung gem. DSGVO und NDSG
Anlage 2f	Vertrag zur Auftragsverarbeitung mit nTp
Anlage 2g	Vertrag zur Auftragsverarbeitung mit SIEMENS
Anlage 2h	Rahmenvereinbarung zur Auftragsverarbeitung personenbezogener Daten (GWDG)

Göttingen,

Für die Georg-August-Universität Göttingen/
Georg-August-Universität Göttingen
Stiftung Öffentlichen Rechts
- Die Präsidentin (kommissarisch) -
Im Auftrag

Marcus Remmers
Leiter der Abteilung IT

Göttingen, 15.02.2021

Für den Personalrat der Georg-August-Universität
Göttingen
(ohne Universitätsmedizin)
- Der Vorsitzende -

Carsten Dolle

Personalrat der
Georg-August-Universität
Humboldtallee 15, 37073 Göttingen

Anlage 1: Systemformular Zutrittssysteme

1. Systembezogene Informationen

Geltungsbereich der Vereinbarung:	☒ Für alle durch den Personalrat vertretenen Beschäftigten der Georg-August-Universität Göttingen Stiftung Öffentlichen Rechts (ohne Universitätsmedizin Göttingen), die die Funktionalität der Zutrittssysteme (SiPort und AEOS) nutzen.
	☐ Für ehemalige Beschäftigte Anmerkungen:
	☒ Für weitere Personenkreise Professor/innen Studierende Beschäftigte der Universitätsmedizin Göttingen (UMG) (separate Dienstvereinbarung der UMG) Externe und Gäste
Betreiber der Systeme:	Abteilung IT der Universität (AEOS) Geschäftsbereich IT der UMG (SiPort) GWDG (IT-Infrastruktur)
Ansprechpartner für diese Vereinbarung:	Infrastrukturelles Gebäudemanagement (GM4) der Universität

2. Gegenstand / betroffene Beschäftigte und Personenkreise (Kurzbeschreibung, Anzahl)

Gegenstand:	Systeme zur Verwaltung und Gewährung von Online- und Offline-Zutritten per Chipkarte / Transponder in den Liegenschaften der Universität (und der Universitätsmedizin).
Beschreibung:	Die Zutrittssysteme erhalten die Personenstammdaten aus zentralen Systemen. Diesen Stammdaten werden in den Kartenstellen der Universität und der Universitätsmedizin die für den Zutritt benötigten Berechtigungen zugeordnet bzw. entzogen. Zukünftig ist die Möglichkeit vorgesehen, dezentralen Einrichtungen die Zuordnung / den Entzug von Berechtigungen in den jeweils genutzten Liegenschaften zu übertragen.
Anzahl:	→ ca. 25 Mitarbeiter/innen: - Gebäudemanagement der Universität mit Planung, –betrieb und Infrastruktur (GM1, GM 3, GM 4) der Universität - Abteilung IT der Universität - Geschäftsbereich IT der UMG - GWDG als Universitätsrechenzentrum → zukünftig weitere Mitarbeiter/innen in den Einrichtungen der Universität bei Einrichtung der dezentralen Profilverwaltung (max. Anzahl entsprechend der Anzahl der Gebäude) → alle Mitarbeiter/innen der Universität, die die Zutrittssysteme nutzen (werden).

3. Ziele des IT-Systems

Vom System zu erfüllende Ziele:	Verwaltung der Zutrittsberechtigungen per Chipkarte / Transponder zur Gewährung bzw. Verweigerung des Zutritts von Personen in den Liegenschaften der Universität und der Universitätsmedizin gemäß einem festgelegten Rollen- und Rechtekonzept. (Zeiterfassung mit Übertragung nach SAP-HR.)
Bezeichnung der betroffenen IT-Services:	Zutrittsregelungen
Beschreibung der vom System wahrzunehmenden Aufgaben und Prozesse:	Automatische Übernahme von Personenstammdaten aus zentralen Quellsystemen. Vergabe und Entzug von Zutrittsberechtigungen für Personen. Steuerung der festgelegten Zutritte an den Endgeräten.
Anmerkungen:	keine

4. Zugrundeliegende / Weitere Vereinbarungen / Bestimmungen

Systemdokumentation:	Bezeichnung: Systemdokumentation Zutrittssystem AEOS In der Version Nr. 1 vom 24.07.2019 (siehe Anlage 2.1) Bezeichnung: Systemdokumentation Zutrittssystem SiPort In der Version Nr. 1.3 vom 02.09.2019 (siehe Anlage 2.2)
Weitere Vereinbarungen / Bestimmungen:	Bezeichnung: Betriebskonzept Zutrittssystem AEOS In der Version Nr. 1 vom 24.07.2019 (siehe Anlage Anlage 2b.1) Bezeichnung: Betriebskonzept Zutrittssystem SiPort In der Version Nr. 1 vom 02.09.2019 (siehe Anlage Anlage 2b.2)

5. An dem System beteiligte Dritte (Externe, Auftragsverarbeitung)

An dem System sind folgende Dritte beteiligt:	UMG als Betreiber SiPort GWDG für den Betrieb der IT-Infrastruktur NEDAP ntp als Lieferant von AEOS SIEMENS als Lieferant von SiPort
Zusatzvereinbarung zur Auftragsverarbeitung:	Rahmenvereinbarung zur Auftragsverarbeitung personenbezogener Daten (gem. Art. 28 EU-DSGVO) mit Datum vom 01.07.2019 mit der GWDG als Universitätsrechenzentrum Vertrag zur Auftragsverarbeitung (gem. Art. 28 DSGVO) mit Datum vom 08.07.2019 mit nTp Vertrag zur Auftragsverarbeitung (gem. Art. 28 DSGVO) mit Datum vom 29.03.2019 mit SIEMENS

6. Eine datenschutzrechtliche Prüfung hat stattgefunden und wird bestätigt:

☐	Ja, es wurde eine Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO durchgeführt. Die geforderten Maßnahmen wurden umgesetzt.
☒	Ja, es wurde eine Verarbeitungstätigkeitsbeschreibung gem. Art. 30 DSGVO erstellt.

7. Vorliegende Dokumente zur datenschutzrechtlichen Prüfung

☐	Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO kann beim Verantwortlichen (Abteilung IT) eingesehen werden. mit Datum vom __.__.2019
☒	Verarbeitungstätigkeitsbeschreibung gem. DSGVO kann beim Verantwortlichen (Abteilung IT) eingesehen werden. mit Datum vom 01.02.2019

8. Sonstige datenschutzrechtliche Regelungen

- Eine Leistungs- oder Verhaltenskontrolle findet nicht statt. Personenbezogene oder personenbeziehbare Daten, die für eine Leistungs- oder Verhaltenskontrolle geeignet sind, dürfen nicht ausgewertet, in andere Systeme übertragen oder dafür verwandt werden, um individuelle Eigenschaften mit Anforderungsprofilen zu vergleichen.
- Das Auslesen oder Auswerten von Ereignisdaten (Historienspeicher) ist nur bei begründetem Verdacht auf schwerwiegenden Missbrauch der Zugangsberechtigung oder auf strafbare Handlungen erlaubt. Der Personalrat ist in jedem Falle zu beteiligen.
- Ein Zugriff auf Protokolldateien oder ein Auslesen bzw. Auswerten von Ereignisdaten, das nicht allein Zwecken der Systemadministration dient, ist nur mit Zustimmung des Personalrats sowie des Datenschutzbeauftragten oder seines Stellvertreters und nur im Beisein eines Mitglieds des Personalrats zulässig.
- Nur bei Gefahr im Verzuge ist stattdessen eine unverzügliche Mitteilung an den Personalrat sowie den Datenschutzbeauftragten oder seinen Stellvertreter vorzunehmen. Wenn diese sich nicht innerhalb einer der Gefahr angemessenen Zeitspanne an der Einsichtnahme in die Zutrittsdaten beteiligen können, darf auch ohne Zustimmung des Datenschutzbeauftragten oder seines Stellvertreters sowie des Personalrates oder zumindest ohne das Beisein eines Mitglieds des Personalrats Einsicht genommen werden. In diesem Fall erhalten der Datenschutzbeauftragte oder sein Stellvertreter und der Personalrat unverzüglich einen ausführlichen Bericht über den Vorfall und die getroffenen Maßnahmen.
- Für sicherheitskritische Bereiche können unter Beachtung von gesetzlichen und universitären Regelungen (DSGVO, NDSG und Informationssicherheitsrichtlinie der Universität Göttingen) abweichende Maßnahmen unter Beteiligung des Personalrates getroffen werden.

9. Löschung personenbezogener Daten

☒	Eine Löschung personenbezogener Daten erfolgt gemäß § 5 IT-RDV.
☐	Eine Löschung erfolgt abweichend von der in § 5 IT-RDV festgesetzten Frist.
	Begründung:

10. Wurde für dieses System im Rahmen der Projektierung ein Konzept für die Schulung der Beschäftigten vereinbart:

☐	Ja, dieses kann beim Personalrat eingesehen werden.
	Betroffene Personen / Rollen:
	Anmerkungen:
☒	Nein
	Begründung: Für die Nutzung der Zutrittssysteme ist keine Schulung für die Anwendung notwendig. Die Schulung der Administratoren und Mitarbeiter/innen des Infrastrukturellen Gebäudemanagement erfolgte durch die Lieferanten im Rahmen der Teststellung und der durchgeführten Workshops. Die Dienststelle stellt sicher, dass – wenn weitergehender Schulungsbedarf u.a. in den dezentralen Einrichtungen besteht – entsprechende Schulungen in der jeweils notwendigen Form bereitgestellt werden können.

11. Wurde für dieses System ein Berechtigungskonzept erstellt:

☒	Ja
	Beschreibung (siehe Anlage 2a): Differenzierung nach Adminstratoren mit vollen Zugriffsrechten, Mitarbeiter/innen des Infrastrukturellen Gebäudemanagement mit Zugriffsrechten für die Verwaltung von Zutrittsrechten sowie zukünftig für Mitarbeiter/innen in den betroffenen Einrichtungen, wenn die Zugriffsrechte dezentral vergeben werden sollen.
☐	Nein
	Begründung:

12. Quellsysteme

SAP HR via IDM, Studierendenverwaltung via IDM

13. Zielsysteme

Daten aus den Zutrittssystemen werden in keiner Form an andere Systeme übergeben.

14. Vorliegende Dokumentationen beim IT-Dienstleister

Zuständiger IT-Dienstleister	Abteilung IT – Informationstechnologie und Informationsmanagement
☒	Systemdokumentation Zutrittssystem AEOS mit Datum vom: 24.07.2019
☒	Systemdokumentation Zutrittssystem SiPort mit Datum vom: 02.09.2019
☒	Differenziertes Berechtigungskonzept Zutrittssysteme mit Datum vom 24.07.2019
☒	Betriebskonzept Zutrittssystem AEOS vom 24.07.2019
☒	Betriebskonzept Zutrittssystem SiPort vom 02.09.2019
☒	Sicherheitskonzept Zutrittssystem AEOS vom 24.07.2019
☒	Verfahrensanweisung Zutrittssystem SiPort vom 24.04.2019

15. Sonstige Bestimmungen, soweit erforderlich

Abgrenzung Datenerhebung außerhalb des Zutritts	Diese Vereinbarung gilt nicht für Daten, die zu einem anderen Zweck als der Regelung eines Zutritts (z.B. Zeiterfassung) erhoben werden, auch wenn dies mit dem gleichen IT-System geschieht. Der Umgang mit diesen Daten wird, auch wenn sie im Zusammenhang mit einem Zutrittssystem oder durch das gleiche IT-System erfasst werden, in gesonderten Dienstvereinbarungen geregelt.