Dienstvereinbarung für den Betrieb eines IT-Servicedesks an der Fachhochschule Südwestfalen (FH SWF)

abgeschlossen zwischen den folgenden Vertragsparteien:

Kanzler der FH SWF

Personalrat der Beschäftigten in Technik und Verwaltung der FH SWF (PR TuV)

Rektor der FH SWF

Personalrat der wissenschaftlich Beschäftigten der FH SWF (PR Wiss)

§ 1 Gegenstand der Dienstvereinbarung

Die Einführung eines IT-Servicedesks ermöglicht eine professionelle und zeitnahe Reaktion auf alle eingehenden Meldungen und Anfragen. Aus diesem Grund wird an der FH SWF im Dezernat 6 „IT-Services" ein sog. „Single Point of Contact (SPOC)" geschaffen, eine zentrale Ansprechstelle im IT-Bereich, welche zentral alle Anfragen und Störungsmeldungen annimmt und bearbeitet. Die FH SWF ist bestrebt, die Anfragen und Störungsmeldungen einheitlich, kompetent und schnellstmöglich zu bearbeiten. Der IT-Servicedesk soll dazu dienen, die Meldungen entgegenzunehmen, zu dokumentieren und an das Lösungsteam (interner Second Level) zu delegieren, mit dem Ziel, den Service schnellstmöglich in vollem Umfang wiederherzustellen. Idealerweise kann der IT-Servicedesk viele Anfragen selbständig direkt lösen. Somit kann Wartezeit reduziert und entsprechend die Kundenzufriedenheit gesteigert werden. Im Rahmen dieser Zielsetzung sollen drei grundlegende Werkzeuge eingeführt werden:

Für eine nachvollziehbare Bearbeitung von Anfragen und Störungsmeldungen sowie zur Koordination der daraus resultierenden Arbeitsabläufe wird ein Ticketsystem benötigt.

Ein weiteres Werkzeug, welches für den Betrieb eines IT-Servicedesks benötigt wird, ist die Callcenter-Telefonie-Lösung, die vom Funktionsumfang weit über die Möglichkeiten der jetzigen klassischen Telefonanlage der FH SWF hinausgeht.

Zusätzlich wird für den zentralen IT-Servicedesk zur effektiven, schnellen und vereinfachten Hilfeleistung eine Fernwartungssoftware benötigt.

Die nachfolgenden Regelungen sind zum einen als generelle Grundlage für den Schutz der IT-Mitarbeiterinnen und IT-Mitarbeiter und der IT-Anwenderinnen und IT-Anwender insbesondere vor elektronischer Überwachung ihrer Leistung und ihres Verhaltens sowie für die Wahrung ihres Grundrechts auf informationelle Selbstbestimmung zu verstehen. Zum anderen sollen die Regelungen die Akzeptanz der Einführung eines zentralen IT-Servicedesks fördern.

§ 2 Geltungsbereich

Diese Dienstvereinbarung gilt für alle Mitarbeiterinnen und Mitarbeiter der FH SWF im Sinne des § 5 LPVG NRW.

§ 3 Beschreibung der eingesetzten Werkzeuge

(1) Das Ticketsystem (Anlage 1) ermöglicht die systematische Erfassung (Empfang, Bestätigung, Klassifizierung, Bearbeitung und Beantwortung) der über verschiedene Medien (z. B. per E-Mail, Telefon oder Webformular) eingehenden Anfragen und Störmeldungen. Durch die Dokumentation im System sind die Bearbeitungsschritte intern nachvollziehbar.

(2) Zur Fernbetreuung bei PC-Problemen wird eine Fernwartungssoftware (Anlagen 2 u. 3) eingeführt. Durch die Einführung der neuen Software soll den IT-Mitarbeiterinnen und IT-Mitarbeitern, die IT-Anwenderinnen und IT-Anwender betreuen, ein Arbeitsmittel zur Verfügung gestellt werden, um bei Bedarf Betreuung mittels Fernwartung leisten zu können. So kann die IT-Mitarbeiterin oder der IT-Mitarbeiter mit dieser Software z. B.
- eine Übersicht über die Hardwarekomponenten und die aktive Software erhalten,
- den Bildschirm angezeigt bekommen,
- Software auf dem Rechner installieren oder deinstallieren,
- Eingriffe in Dateien vornehmen (z.B. Konfigurationsdateien übertragen),
- steuernd in den Dialog eingreifen,
- den gesteuerten Rechner neu starten und
- die Bedienung kontrolliert übernehmen.

(3) Die Callcenter-Telefonie-Lösung (Anlage 4) ermöglicht die Erreichbarkeit des IT-Servicedesks unter einer einheitlichen Rufnummer mit Warteschlangenfunktionalität.
Die wichtigsten Funktionen sind:
- Warteschlangenfunktionalität inkl. individueller Ansagen und Wartemusik
- Anrufweiterschaltung
- Zeitsteuerung der Erreichbarkeit (z.B. Weiterleitung auf Sprachspeicher außerhalb der Verfügbarkeitszeiten des IT-Servicedesks)
- Eingehende und ausgehende Telefonate zwischen öffentlichem Telefonnetz und dem Wissenschaftsnetz (Breakin – Breakout)
- Konferenzschaltung
- Rufgruppen inkl. Signalisierung am Gerät
- Flexible Arbeitsplatzwahl (Anmelden an verschiedenen Endgeräten möglich)
- Anruflisten
- Sprachansagen / Sprachspeicher

§ 4 Rechtsgrundlage der Verarbeitung personenbezogener Daten

(1) In den in § 3 aufgeführten Systemen werden personenbezogene Daten verarbeitet. Die Inhalte ergeben sich aus dem Verzeichnis von Verarbeitungstätigkeiten. Rechtsgrundlage für die Verarbeitung ist Art. 6 Abs. 1 Satz 1 lit. e) DSGVO i.V.m. § 3 Abs. 1 DSG NRW. Der Betrieb des IT-Servicedesks erfolgt zur Wahrnehmung einer Aufgabe der verarbeitenden Stelle in Form der Bereithaltung einer funktionierenden IT-Infrastruktur. Diese liegt im öffentlichen Interesse, da sie der sparsamen und wirtschaftlichen Verwendung der der Hochschule zur Verfügung stehenden Ressourcen dient. Die schutzwürdigen Belange der Betroffenen sind dabei immer zu berücksichtigen. Dafür ist unabdingbar, dass hinsichtlich der Aktivitäten zur Fernbetreuung bei PC-Problemen (§ 3 Abs. 2) die Fernbetreuung nur mit Zustimmung der IT-Anwenderin oder des IT-Anwenders erfolgt, diese/r anwesend ist und für diese/n jederzeit die Möglichkeit besteht, die Fernbetreuung zu beenden.

(2) Personenbezogene Auswertungen finden nicht statt.

§ 5 Servicezeit

Die Servicezeit orientiert sich an dem Bedarf und wird auf den Internetseiten des IT-Service bekannt gegeben.

§ 6 Verbot der Verhaltens- oder Leistungskontrolle

Die Nutzung des Ticketsystems, der Fernwartungssoftware und der Callcenter-Telefonie-Lösung darf nicht, auch nicht im Wege des Profiling, zur Verhaltens- oder Leistungskontrolle der IT-Mitarbeiterinnen und IT-Mitarbeiter und der IT-Anwenderinnen und IT-Anwender genutzt werden. Dies bezieht sich sowohl auf die Inhalte (Nutzungsdaten) als auch auf die durch die Nutzung entstehenden Protokolldaten (Verkehrsdaten).

§ 7 Datenschutz

(1) Es wird besonderer Wert auf den Schutz und die Sicherheit der personenbezogenen Daten gelegt. Passwörter sind geheim zu halten, es darf keine Weitergabe an Vorgesetzte oder andere Beschäftigte erfolgen.

(2) Der Einzelperson darf durch ihre Festlegung der Vergaberechte auf ihre persönlichen Anwendungsdaten kein dienstlicher Nachteil entstehen.

(3) Die Zugriffsrechte sind so transparent zu gestalten, dass jede Person feststellen kann, welche anderen Personen Zugriff auf die von ihr freigegebenen Daten haben.

§ 8 Rechte und Pflichten der Beschäftigten

(1) Die Beschäftigten haben im Rahmen der DSGVO und des DSG NRW das Recht auf Auskunft über alle über sie gespeicherten Daten sowie das Recht auf Berichtigung und auf Löschung.

(2) Erfolgen notwendige Eingriffe (inklusive Fernwartung) der jeweils zuständigen IT-Mitarbeiterinnen und IT-Mitarbeiter an Arbeitsplatzrechnern von IT-Anwenderinnen und IT-Anwendern, so ist ihnen das vorher anzuzeigen. Außerdem sind sie vorab über den Ablauf des Eingriffs zu informieren und auf ihre Rechte und Pflichten zur datenschutzgerechten Durchführung des Eingriffs hinzuweisen, insbesondere darauf, dass sie auf ihrem Bildschirm befindliche Anwendungen mit personenbezogenen Daten schließen müssen und wie sie den Eingriff beenden können.

(3) Die IT-Mitarbeiterinnen und IT-Mitarbeiter sowie die IT-Anwenderinnen und IT-Anwender werden von der Dienststelle ausdrücklich verpflichtet, über die ihnen zugänglichen personenbezogenen und -beziehbaren Daten, auch über die Leistung und das Verhalten von Beschäftigten Stillschweigen zu bewahren. Insbesondere dürfen IT-Mitarbeiterinnen und IT-Mitarbeiter, die dienstlichen Zugang zu personenbezogenen Daten haben, solche Daten nicht unbefugt zu einem anderen als dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck verarbeiten oder offenbaren; dies gilt auch nach Beendigung der Tätigkeit. Sie werden hinsichtlich der Einhaltung des Fernmeldegeheimnisses und Datenschutzes geschult und auf die rechtlichen Konsequenzen hingewiesen. Die Datenschutzrichtlinie der Fachhochschule Südwestfalen ist einzuhalten.

(4) Personelle Maßnahmen, die auf Informationen beruhen, die unter Verletzung dieser Dienstvereinbarung gewonnen wurden, sind unwirksam und unverzüglich rückgängig zu machen.

§ 9 Rechte der Personalräte

Bis zu zwei Vertreterinnen oder Vertreter je Personalrat haben zum Zweck der Prüfung der Einhaltung dieser Dienstvereinbarung unter Berücksichtigung der jeweils geltenden Sicherheitsbestimmungen und betrieblichen Belange nach vorheriger rechtzeitiger Anzeige das Recht, sich die Funktionsweise der IT durch Verantwortliche erklären und demonstrieren zu lassen. Dazu gehören auch die Möglichkeiten, Programme aufrufen und sich die Erfassungs- und Ausgabemasken anzeigen oder sich die direkte Arbeit mit dem System zeigen zu lassen. Diese Möglichkeiten bedeuten nicht, dass beispielsweise Datensicherungsläufe, Jahresabschlusslauf, Datenreorganisation, Systemgenerierung oder ähnliches für die Überprüfung zu unterbrechen sind, da diese betrieblichen Belange vorrangig zu berücksichtigen sind. Alle Beschäftigten sind hierbei hinsichtlich der von ihnen angewandten IT gegenüber dem Personalrat auskunftsberechtigt und -verpflichtet. Dabei gegebene Auskünfte dürfen den Beschäftigten nicht

zum Nachteil gereichen. Alle zum System gehörenden Handbücher und Systemunterlagen sind den Personalräten auf Wunsch in der aktuellen Version zeitweise zu überlassen.

§ 10 Systemdokumentation

Die Systemdokumentation ist stets auf dem aktuellen Stand zu halten.

§ 11 Aus- und Weiterbildung

Die Dienststelle bietet ausreichende Informationen und Hilfematerialien sowie nach Bedarf Schulungen zur Nutzung der eingesetzten Systeme an.

§ 12 Inkrafttreten, Kündigung, Nachwirkung

(1) Diese Dienstvereinbarung tritt am Tag ihrer Unterzeichnung in Kraft.

(2) Diese Dienstvereinbarung kann einvernehmlich geändert werden. Änderungen bedürfen der Schriftform.

(3) Diese Dienstvereinbarung kann von jeder Vertragspartei mit einer Frist von drei Monaten zum Ende eines Kalenderjahres gekündigt werden. Die Kündigung bedarf der Schriftform.

(4) Nach Eingang der Kündigung sind unverzüglich Verhandlungen über eine neue Dienstvereinbarung aufzunehmen.

(5) Für den Fall einer Kündigung dieser Dienstvereinbarung beträgt die Nachwirkung ein Jahr.

Anlagen:

1. OTRS Handbuch
2. FastViewer Handbuch
3. FastViewer Sicherheitskonzept
4. Callcenter-Telefonie-Lösung Handbuch
5. Verzeichnis von Verarbeitungstätigkeiten
   a. OTRS Ticketsystem
   b. FastViewer Fernwartungstool
   c. Callcenter-Telefonie-Lösung „VoIP-Centrex"
6 Qualifizierungskonzept

Iserlohn, den 27.06.2019

Heinz-Joachim Henkemeier
Kanzler

Iserlohn, den 26.06.2019

Harald Jakob
Vors. PR TuV

Iserlohn, den 26.06.2019

Prof. Dr. Claus Schuster
Rektor

Iserlohn, den 26.06.2019

Bernadette Stolle
Vors. PR Wiss

Anlage 1

OTRS Handbuch

ftp://ftp.otrs.org/pub/otrs/doc/doc-admin/6.0/de/pdf/otrs_admin_book.pdf

Anlage 2

FastViewer Handbuch

https://fastviewer.com/demo/FastViewer_Handbuch.pdf

Anlage 3

Die Technische Universität Dortmund betreibt die Fernwartungssoftware FastViewer im eigenen Rechenzentrum (ITMC) und bietet anderen Hochschulen die Nutzung als Service an. Das Sicherheitskonzept der TU Dortmund lautet wie folgt:

FastViewer Sicherheitskonzept der TU Dortmund

1. Generelle Systembeschreibung

FastViewer ist ein Support- und Fernwartungstool, mit dem durch Fernzugriff Beratung und Fehlerbehebungen auf Anwenderseite unterstützt werden. Mit dem FastViewer kann vor allem der Bildschirminhalt eines Computers zu einem anderen Computer übertragen werden. Dadurch ist es möglich, dass Administratoren und Systemnutzer, die sich an verschiedenen Orten aufhalten, gemeinsam den Desktop des Nutzers betrachten. Während sie miteinander telefonieren, können sie sich gegenseitig Dokumente oder Anwendungen zeigen. Der Zweck des Systems ist, dass Mitarbeiter des Supports Fehler in Softwareprodukten beheben oder Unterstützung bei deren Einsatz geben können, ohne sich selbst an den Computer zu begeben, an dem die Störung aufgetreten ist bzw. die Hilfe benötigt wird.

FastViewer besteht aus mehreren Komponenten: Die FastViewer-Support Software wird auf dem Rechner des Supports gestartet und ermöglicht die Initiierung des Verbindungsaufbaus, die Anzeige des Bildschirminhalts des Kunden und die Steuerung des Kundenrechners, jeweils wenn das durch den Kunden autorisiert wurde.

Die Klientensoftware wird auf dem Rechner gestartet, auf dem ein Problem aufgetreten ist. Die Software muss durch den Nutzer aktiv gestartet werden, der Verbindungsaufbau ist nur unter aktiver Beteiligung des Nutzers möglich und es sind nach Bestätigung verschiedene Eskalationsstufen von Berechtigungen möglich. Durch den Nutzer kann jederzeit während einer Sitzung die Berechtigung auch wieder entzogen werden.

Der FastViewer-Server sichert und protokolliert die Verbindung. Berechtigungen von Beratern werden geprüft, der Verbindungsaufbau findet über den Server gesichert statt. Laut Aussage des Herstellers kann an dem Server die Verbindung nicht inhaltlich überwacht werden. Die Übertragung zwischen Client und Berater erfolgt Ende zu Ende verschlüsselt.

Der Ablauf der Nutzung und einer Beratungssitzung ist in der beigefügten Abbildung dargestellt.

Das Produkt ist hinsichtlich der Sicherheitsmechanismen unabhängig überprüft worden, was durch Zertifizierungen belegt ist. Die Nutzung erscheint für die Betroffenen in jedem Zustand an der Oberfläche nachvollziehbar, was gleichzeitig bedeutet, dass die Administratoren wiederum für die Betroffenen erkennbar handeln. Ein Kopieren oder Einsehen von Daten beispielsweise ohne Kenntnis des Kunden erscheint nicht möglich.

In die Abwägung zum Einsatz des Systems ist zu berücksichtigen, dass unter Nutzung des Systems zeitnah kompetente Beratung und Unterstützung angeboten werden kann, was in einigen Bereichen andernfalls nicht gegeben ist. In diesen Fällen ist auch davon auszugehen, dass sich die Sicherheit der angeschlossenen Systeme verbessert, weil (Sicherheits-)Probleme schneller erkannt und behoben werden.

2. Angriffs- und Schadensszenarien

Dieses Dokument beschreibt Maßnahmen, die technisch und organisatorisch getroffen wurden, um die personenbezogenen Daten im System FastViewer zu schützen. Dazu sollten zunächst die Angriffs- und Schadensszenarien benannt werden. Auf eine detaillierte Darstellung und Bewertung der Eintrittswahrscheinlichkeiten wird hier verzichtet.

- *Szenario 1: Unberechtigter Zugriff/Manipulation des Systems (bekannte Passwörter, physischer Zugriff)*
- *Szenario 2: Abhören und Manipulation des Netzverkehrs*
- *Szenario 3: Übernahme und Abhören von Clients*
- *Szenario 4: Datenversand oder kopieren auf externen Datenträgern*

Die Maßnahmen umfassen entsprechende vorbeugende Maßnahmen, Maßnahmen zur Erkennung von Problemen und Maßnahmen zur Reaktion auf diese Szenarien.

3. Sicherheits-Eigenschaften von FastViewer

Die komplette Sitzung ist Servergesteuert. Die Datenübertragung wird mit dem 256-Bit-AES-Schlüssel (verwendet den Rjindeal-Algorithmus) verschlüsselt. Dem FastViewer-Kommunikationsserver ist es NICHT möglich die Daten zu entschlüsseln, da er zu keinem Zeitpunkt im Besitz des 256-Bit-AES Schlüssels ist (TÜV Zertifikat wird jährlich aktualisiert).

Das Clientprogramm wird bei der Kompilierung mit einer Prüfsumme versehen (CRC Prüfung) Wird diese nun über ein Tool geändert bzw. gehackt, ist das Programm aufgrund eines Prüfsummenfehlers nicht mehr startbar. Dies verhindert effektiv eine unerwünschte Veränderung am Programmcode und stellt die Funktionstüchtigkeit aller definierten Sicherheitsfeatures sicher. Es findet keine Installation eines Programmes/Modul auf dem Client statt. Nach einer Fernwartungssitzung werden die Programmodule rückstandsfrei beendet. Dies bewirkt, dass keine Eingriffe im Kundensystem vorgenommen werden können und spätere Zugriffsmöglichkeiten auf dem entfernten System nicht gegeben sind. Die Clientprogramm wird nur mit einer signierten Mail versendet. In dieser Mail wird auch darauf hingewiesen, dass keine FastViewer Programme auf einem anderen Wege oder von unsignierten Absendern an die Clients gesendet werden.

Transparenzmaßnahmen
Der Start der Sitzung erfolgt durch die Initiative des Nutzers. Administratoren sind angehalten keine Sitzung zu starten. Damit wird vermieden das Dritte sich als Administrator ausgeben können und eine Sitzung starten. Jede Aktion muss vom Client bei den Sitzungen erneut freigegeben werden. Der Client User kann die ganze Zeit sehen was an seinem Computer gemacht wird. Nach einer Sitzung wird ein umfangreiches Log zur Verfügung gestellt, welches Rückschlüsse auf die Dauer (Beginn und Ende), Hostnamen sowie beteiligte IP-Adressen zulässt. Dieses Log lässt sich zu Auswertungszwecken exportieren. Auf Seiten des Kunden sowie als auch des Supporters kann zu Nachweiszwecken eine Videoaufzeichnung aktiviert werden. Die Videodatei wird revisionssicher an den Player in einem eigenen Format gekoppelt und als eigenständiges EXE-File ausgegeben. Dies verhindert eine spätere Manipulation.

4. Maßnahmen

Räumliche Absicherung der Server

Server befinden sich in einem gesicherten Raum:

Maßnahmen sind im übergreifenden Sicherheitskonzept dargestellt.

Servertechnik

Es werden nur Server namhafter Hersteller mit Qualitätsmerkmalen eingesetzt, die auf Ausfallsicherheit (Fehlertolerante, fehlererkennende Hardware, Redundanz von kritischen Komponenten, Netzwerkperformance) ausgelegt sind. Das System läuft am virtueller Server auf dem TU System. Weitere Maßnahmen dazu sind im übergreifenden Sicherheitskonzept dargestellt.

Die Administration erfolgt durch die Systemverwalter des Serviceteam.

Nutzerberechtigung

Die Nutzung oder das Starten des Mastermodul, zum Start einer Sitzung, wird über die eigene Nutzerverwaltung im FastViewer ermöglicht. Ablauf zum Eintragen des Beraters: Nach der Einweisung und Belehrung des Beraters gemäß des Verfahrens Verzeichnis und diesem Dokument, wird der Berater in der zentralen Nutzerverwaltung des FastViewer Servers von den benannten Administratoren (siehe Weitere Maßnahmen) eingetragen. Nicht eingetragene Berater können somit keine Beratungssitzung aufrufen.

Netzsicherheit

Übergreifende Maßnahmen sind im allgemeinen dargestellt.

Der Server läuft in einem speziell geschützten Netzwerk, in dem keine Standarduser Zugang haben. Jeder Server in diesem Netzwerk hat in der zentralen Firewall nur die für Ihn bestimmten Dienste/Ports freigegeben. Am Server selbst ist auch eine Firewall aktiv. Administrativen Zugang zum Server haben nur die Systemverwalter. Die nutzenden Berater haben keine Möglichkeit auf den Server zuzugreifen.

(Diese Maßnahmen wirken den Szenarien 1, 2, und 3 entgegen.)

Sicherung der Admin -Clients

- *Alle Rechner der Administratoren sind gemäß Abschnitt 3 des allgemeinen Sicherheitskonzepts konfiguriert. (Diese Maßnahmen wirken den Szenarien 1 bis 4 entgegen.)*

Protokollierungen

Folgende Protokolle werden zur Datensicherung erhoben:

- ***Datenbankprotokoll***

Die Protokolle werden ¼ Jahr aufbewahrt. Die Aufbewahrung hängt mit dem Plattenplatz zusammen.

- ***Anmeldeprotokolle*** *(Fehlerhafte Anmeldeversuche werden am Server festgehalten. Diese Protokolle werden alle 2 Tage nach einer Blickkontrolle wieder gelöscht.)*

- ***Netzwerkprotokolle*** *(Die Firewall überwacht den Datenverkehr anonym – weitere Ausführungen siehe Anhang Firewall)*

- ***Sicherheitstechnische Kontrolle der IT-Landschaft*** *(Mit Hilfe der Software „Quick Check Security Audit“ wird in regelmäßigen Abständen von etwa 1 Monate die IT-Landschaft kontrolliert. Die entstandenen Protokolle werden entsprechend vom sic des ITMC aufbewahrt.*

Die Protokolle werden zu Sicherungszwecken erhoben und sind gemäß § 19 Abs. 2 d gegen die anderweitige Nutzung gesperrt.

(Durch diese Maßnahmen wird vor allem den Szenarien 1 und 3 entgegengewirkt.)

Konfigurationseinstellungen von FastViewer

Standalone Windows 20xx Server mit eigener Nutzerverwaltung

Lokale Firewall aktiv

Incoming Port 5000 freigegeben mit Kopplung an FastViewer

Outgoing keine Freigabe

Überwachung über zentralen NAGIOS Dienst des Plattenplatzes und der Serverauslastung

FastViewer wird als Komplettprodukt mit Datenbank geliefert und installiert

Die Beraterzugänge sind in der Datenbank des FastViewer gespeichert

Weitere Maßnahmen

Alle Mitarbeiter, die mit FastViewer arbeiten, sind schriftlich zur Verschwiegenheit verpflichtet und hinsichtlich der rechtlichen Folgen belehrt worden.

Folgende Personen haben Administrationsberechtigungen für Server und Datenbanken von FastViewer:

Server: .	*Systemteam TU Dortmund ITMC*
Datenbank:	*wie Server und DB..*

Ablauf Useranfrage über Fastviewer siehe Seite 14

Anlage 4

Callcenter-Telefonie-Lösung „VoIP-Centrex“

https://voip-centrex.dfn.de/de/handbuecher/portale/serviceportal/handbuch-serviceportal/

Anlage 5

Verzeichnis der Verarbeitungstätigkeiten siehe ab Seite 15

Anlage 6

Schulungskonzept

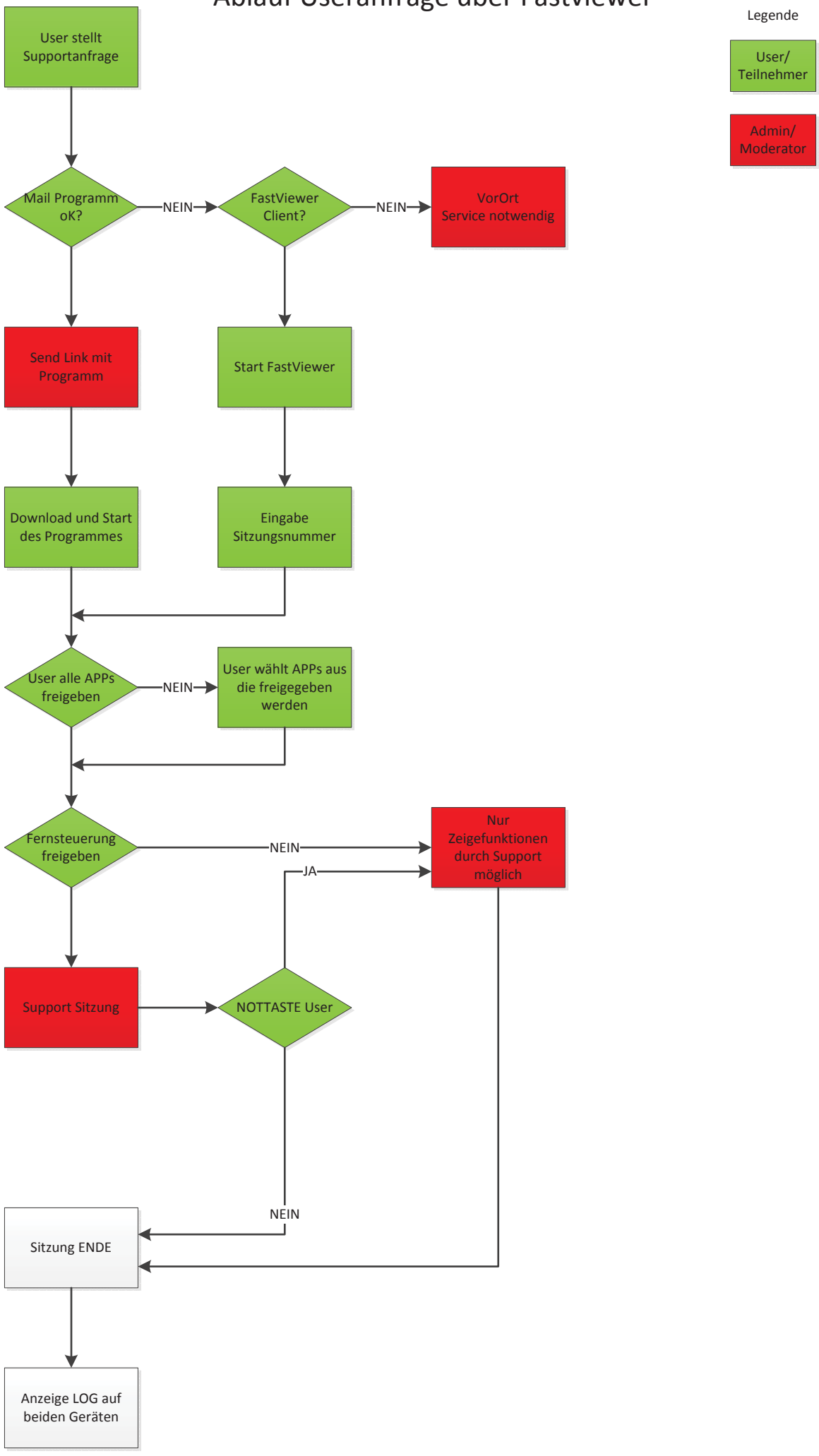
Um zu gewährleisten, dass alle IT-Mitarbeiterinnen und IT-Mitarbeiter sicher im Umgang mit den benötigten Tools sind, unterscheidet das Schulungskonzept folgende Maßnahmen:

- Anwender-Schulungen
  Vor der Arbeit mit den Tools erhalten alle IT-Mitarbeiterinnen und IT-Mitarbeiter eine Anwenderschulung.
  Ziel: IT-Support mit Hilfe der Tools durchführen zu können
  Zielgruppe: IT-Mitarbeiterinnen und IT-Mitarbeiter
  Dauer: ca. 1 Tag
  Durchführung: Intern (IT-Services SG 6.3)

- Update-Schulungen
  Für den Fall, dass sich die Tools durch das Einspielen einer neuen Version (Update) ändern, werden die IT-Mitarbeiterinnen und IT-Mitarbeiter über die Veränderungen informiert.
  Ziel: Veränderungen kennen und neue Funktionen anwenden können
  Zielgruppe: IT-Mitarbeiterinnen und IT-Mitarbeiter
  Dauer: ca. 1 Tag
  Durchführung: Intern (IT-Services SG 6.3)

Wenn IT-Mitarbeiterinnen und IT-Mitarbeiter nicht an Schulungen teilnehmen konnten oder ein weitergehender Schulungsbedarf besteht, werden soweit möglich Ersatztermine angeboten oder additiv Schulungen durch das Sachgebiet 6.3 durchgeführt.

Ablauf Useranfrage über Fastviewer



Verzeichnis von Verarbeitungstätigkeiten

des Verantwortlichen gemäß Art. 30 Abs. 1 DS-GVO

- Besonderer Teil * -

Datum

Az. (intern)

☒ Neue Verarbeitungstätigkeit

☐ Änderung bestehender Verarbeitungstätigkeit

1 Bezeichnung der Verarbeitungstätigkeit[1]

Bezeichnung der Verarbeitungstätigkeit	IT-Servicedesk OTRS Ticketsystem
Zweck der Verarbeitung	Betrieb eines zentralen IT-Servicedesks der FH SWF zur Beantwortung von Anwenderfragen und Beseitigung von technischen Problemen bzgl. der Hochschul-IT

2 Innerorganisatorische Ansprechpartner[2]

Verantwortliche Fachabteilung	IT-Services
Fachlicher Ansprechpartner	Frau Fatma Mutlu
Telefon	02371 – 566 2646
E-Mail-Adresse	mutlu.fatma@fh-swf.de
Technischer Ansprechpartner	Frau Fatma Mutlu
Telefon	02371 – 566 2646
E-Mail-Adresse	mutlu.fatma@fh-swf.de

3 Angaben zum ggf. mit dem Verantwortlichen gemeinsam Verantwortlichen[1]

Name

Straße

PLZ, Ort

* [1,2] Hinweis: Bei Angaben, die im Folgenden mit ([1]) gekennzeichnet sind, handelt es sich um solche, die gemäß Art. 30 DS-GVO zwingender Bestandteil des VVT sein müssen. Angaben, die im Folgenden mit ([2]) gekennzeichnet sind, sind solche, die aus Gründen der Rechenschaftspflicht gemäß Art. 5 Abs. 2 DS-GVO notwendig sind. Weitere Informationen dazu finden Sie in unseren Ausfüllhinweisen.

Land _____

Telefon _____

E-Mail-Adresse _____

4 Beschreibung der Verarbeitungstätigkeit[2]

Das OTRS Ticketsystem dient der systematischen Erfassung, Bearbeitung und Dokumentation eingehender Anfragen und Störmeldungen. Im Ticketsystem werden allgemeine Stammdaten wie Name, Vorname und die E-Mail-Adresse gespeichert. Diese Daten werden vom IT-Anwender während einer Anfrage abgefragt. Diese Daten werden ausschließlich zur Kontaktaufnahme mit dem IT-Anwender genutzt.

Darüber hinaus können Daten, die im Rahmen der Problembeschreibung entstehen, wie z.B. Angabe der Matrikelnummer, Benutzername, Dateiuploads, private E-Mail-Adresse, (Fach-)Bereich gespeichert werden.

5 Kategorien personenbezogener Daten[1]

In der Spalte Bes. ist ein „x“ zu setzen, wenn das jeweilige Datum einer besonderen Kategorie personenbezogener Daten gemäß Art. 9 DS-GVO oder Art. 10 DS-GVO zuzuordnen ist.

Lfd. Nr	Beschreibung	Bes.
1	Daten die vom Kunden an das Ticketsystem übermittelt werden: Störmeldungen bzw. Supportanfragen: Beschreibung des Anliegens (i.d.R. Problembeschreibungen) sowie Zusammenfassung der Beschreibung.	
2	Daten die vom 1st bzw. 2nd Level Support übermittelt werden: Lösungsvorschläge sowie weitere dazugehörige relevante Informationen: Status, Auswirkung und Dringlichkeit	
3	Daten die systemtechnisch übermittelt werden: Benutzerdaten (Beschäftigte) bestehend aus - Name, Vorname, Mail-Account - E-Mail-Adresse, Rufnummer, Faxnummer - Beschäftigungsstelle - Adresse Benutzerdaten (Studierende) bestehend aus - Name, Vorname, Mail-Account - E-Mail-Adresse	
4	Daten die systemtechnisch erzeugt werden: Zeitstempel: Zeitpunkt der Anfrage und Lösungszeitpunkt; Merkmale zur eindeutigen Zuordnung von Datensätzen: verantwortliche Person und verantwortliche Rolle; Verknüpfte Objekte: Zusammengeführte Störungen	

Hinweis: Erfolgt eine umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten, so ist eine Datenschutz-Folgenabschätzung (siehe Ziffer 13) durchzuführen.

6 Kategorien betroffener Personen[1]

Lfd. Nr. aus 5.	Betroffene
1, 3, 4	Angehörige der Hochschule (Beschäftigte und Studierende)
2, 3, 4	Angehörige der IT-Services
1 - 4	Administratoren des OTRS Ticketsystems

7 Rechtsgrundlage der Verarbeitungstätigkeit[2]

Lfd. Nr. aus 5.	Bezeichnung der Vorschrift(en) oder Hinweis auf **Einwilligung** (Einwilligungstext bitte als Anhang beifügen)	Erläuterungen
1 - 4	Art. 6 Abs. 1 Satz 1 lit.e) DSGVO i.V.m. § 3 Abs. 1 DSG NRW und Dienstvereinbarung für den Betrieb eines IT-Servicedesks an der FH SWF	

8 Empfänger personenbezogener Daten[1]

8.1 Interne Empfänger innerhalb der Organisation des Verantwortlichen

Lfd. Nr. aus 5.	Interne Stelle	Zweck
1 - 4	Registrierte Nutzer des Systems (IT-Services MA)	Anfragenbearbeitung
1 - 4	Administratoren	Administration des Systems

8.2 Externe Empfänger

In der Spalte ADV ist ein „x“ zu setzen, wenn der Empfänger im Rahmen einer Auftragsverarbeitung tätig wird. Dann ist beim Zweck der Tätigkeitsumfang zu beschreiben.

Lfd. Nr. aus 5.	Empfänger, i.d.R. mit ladungsfähiger Anschrift	Zweck bzw. Tätigkeit	ADV

Sofern Empfänger ihren Sitz in einem Drittland haben oder es sich um eine internationale Organisation handelt:

Empfänger aus 8.2. mit Bezeichnung des Drittlandes	Die Weitergabe wird gestützt auf
	☐ einen Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DS-GVO), ☐ die Herstellung eines ausreichenden Datenschutzniveaus durch verbindliche interne Datenschutzvorschriften (Art. 46 Abs. 2 lit. b i.V.m. 47 DS-GVO, ☐ die Herstellung eines ausreichenden Datenschutzniveaus durch Standarddatenschutzklauseln (Art. 46 Abs. 2 litt. c und d DS-GVO, ☐ die Herstellung eines ausreichenden Datenschutzniveaus durch genehmigte Verhaltensregeln (Art. 46 Abs. 2 lit. e i.V.m. 40 DS-GVO, ☐ die Herstellung eines ausreichenden Datenschutzniveaus

	durch ein Zertifizierungsmechanismus (Art. 46 Abs. 2 lit. f i.V.m. 42 DS-GVO), ☐ die Herstellung eines ausreichenden Datenschutzniveaus durch folgende sonstige Maßnahmen (Art. 46 Abs. 2 lit. a, Abs. 3 litt. a und b DS-GVO): ☐ folgenden Ausnahmetatbestand des Art. 49 DS-GVO:

9 Zugriffsberechtigte Personengruppen oder Personen, die allein zugriffsberechtigt sind[2]

Lfd. Nr. aus 5.	Personen(gruppe)	Umfang
1 - 4	Administratoren des OTRS Ticketsystems (Ausgewählter Personenkreis IT-Services)	
1 - 4	„2nd – Level“ Support (Mitarbeiter im operativen Tätigkeitsfeld des IT-Services)	
1 - 4	„1st – Level“ Support (Ausgewählter Personenkreis IT-Services und IT-Servicedesk)	

10 Fristen für die Löschung[1]

Lfd. Nr. aus 5.	Frist
1 - 4	ggf. unterschiedliche Löschfristen für einzelne Datenarten aufführen
1 - 4	Tickets werden grundsätzlich nicht gelöscht, sondern nach ca. einem Jahr pseudonymisiert und anschließend archiviert

11 Allgemeine Beschreibung der eingesetzten Hardware, Software und der Vernetzung[2]

11.1 Eingesetzte Software auf Klienten und Servern außer dem Betriebssystem

Lfd. Nr.	Art der Software	Bezeichnung	Version	Einsatz
1	Anwendungssoftware	OTRS (Open Technologie real Services) - Ticketsystem	6	☐ Klient ☒ Server

11.2 Beteiligte Klienten (Arbeitsplatzrechner, mobile Rechner, Terminal, Videokamera usw.)

☒ Es handelt sich um eine Webanwendung, bei der die Klienten nicht näher bestimmbar sind

Anzahl	Typ	Betriebssystem, Version	Software, lfd. Nr. aus 11.1	Netzwerk & Hardware	Daten, lfd, Nr. aus 5.
Alle Clients des Dez. 6	Arbeitsplatzrechner	Windows, Linux, Internetbrowser usw.		☒ IPv4 ☐ IPv6 ☐ SSD-Festplatte ☐ Ext. Medium	1 – 4
Alle mobilen Geräte des Dez. 6	Mobile Geräte	Android, Apple IOS, Microsoft, Linux, Internetbrowser usw.		☒ IPv4 ☐ IPv6 ☐ SSD-Festplatte ☐ Ext. Medium	1 - 4

11.3 Beteiligte Server

Lfd. Nr.	Funktion	Betriebssystem, Version, Virtualisierung	Software, lfd. Nr. aus 11.1	Hardware	Standort	Daten, lfd. Nr. aus 5.
1	Webserver mit Datenbank Backend	☒ virtualisiert	1	☐ SSD-Festplatte	Ort/Firma: ☐ extern ☒ intern	1 - 4

11.4 Datensicherung

Lfd.	Medium	Server, lfd.	Software, lfd.	Aufbewahrungsort	Daten,

Nr.		Nr. aus 11.3	Nr. aus 11.1		lfd. Nr. aus 5.
1	Datensicherung innerhalb des Storage Systems (NetApp)	1	1	Iserlohn Datacenter	1 - 4

11.5 Darstellung der Netzstruktur

☒ Ist als folgende Anlage beigefügt: Anlage 1

11.6 Verwendete Protokolle, Dienste und Verschlüsselung

Übertragungsabschnitt	Software, lfd. Nr. aus 11.1	Protokoll, Port	Verschlüsselung
Client <->Server	1	https/443 smtps/587 bzw. 465 ssh/22	https/443 ja smtps ja ssh/22 ja

12 Technische und organisatorische Maßnahmen[1]

☐ Es wird auf folgendes Dokument verwiesen:

☒ Es sind (ggf. zusätzlich) folgende Maßnahmen getroffen:

12.1 Pseudonymisierung

Siehe Abschnitt 10

12.2 Verschlüsselung

Die Kommunikation zwischen Client und Server ist verschlüsselt (siehe 11.6).

12.3 Gewährleistung der Vertraulichkeit

Vertraulichkeit ist gegeben, wenn nur Befugte personenbezogene Daten zur Kenntnis nehmen können, z.B.:

- Zutrittskontrolle durch technische Maßnahmen in gesicherten Räumen, Einbau von Sicherheitsschlössern
- Benutzerkontrolle durch Passwortregelung zur Legitimation
- Zugriffskontrolle durch Vergabe unterschiedlicher Berechtigungen und differenzierter Zugriffsmöglichkeiten auf einzelne Felder

12.4 Gewährleistung der Integrität

Integrität ist gegeben, wenn personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben, z.B.:

- Vermeidung unbefugter oder zufälliger Datenverarbeitung durch Sperre des Zugriffs auf Betriebssysteme und/oder Verschlüsselung der Daten
- Regelmäßige Kontrolle der Aktualität

12.5 Gewährleistung der Verfügbarkeit

Verfügbarkeit ist gegeben, wenn personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können, z.B.:

- Klare und übersichtliche Ordnung des Datenbestandes
- Vergabe von Zugriffsbefugnissen im erforderlichen Umfang (Unter Abwägung gegenüber dem Gebot der Vertraulichkeit)

12.6 Gewährleistung der Belastbarkeit der Systeme

Keine Angaben

12.7 Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall

Siehe Backup-Konzept der Fachhochschule Südwestfalen

12.8 Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

12.9 Weitere Maßnahmen:

☒ Sensibilisierung und/oder Schulung der an Verarbeitungsvorgängen Beteiligten
☒ Beteiligung des/der zuständigen Datenschutzbeauftragten
☒ Hinweis/Verpflichtung der an Verarbeitungsvorgängen Beteiligten auf das Datengeheimnis
☐ Folgende Maßnahmen, die die nachträgliche Überprüfung und Feststellung

gewährleisten, ob und von wem personenbezogene Daten erfasst, verändert oder gelöscht worden sind:

☐ Im Falle einer Übermittlung oder Zweckänderung:
Folgende spezifischen Verfahrensregelungen werden getroffen, um die Einhaltung des LDSG und der DS-GVO sicherzustellen:

☐ Sonstiges:

12.10 Weitere Dokumente:

☐ Interne Verhaltensregeln
☐ Risikoanalyse
☐ Allgemeine Datensicherheitsbeschreibung
☐ Umfassendes Datensicherheitskonzept
☐ Wiederanlaufkonzept
☐ Zertifikat:
Zertifizierungsstelle:
☐ Sonstiges:

13 Datenschutz-Folgenabschätzung[2]

☐ Eine Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO ist notwendig (insbesondere immer notwendig, wenn eine umfangreiche Verarbeitung besonderer Kategorien personenbezogener Daten erfolgt).

☒ Eine Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO ist nicht notwendig.

Verzeichnis von Verarbeitungstätigkeiten

des Verantwortlichen gemäß Art. 30 Abs. 1 DS-GVO

- Besonderer Teil * -

Datum

Az. (intern)

☒ Neue Verarbeitungstätigkeit

☐ Änderung bestehender Verarbeitungstätigkeit

1 Bezeichnung der Verarbeitungstätigkeit[1]

Bezeichnung der Verarbeitungstätigkeit	IT-Servicedesk Callcenter-Telefonie-Lösung VoIP-Centrex
Zweck der Verarbeitung	Zur Betriebsaufnahme des IT-Servicedesks wird von Beginn an eine Callcenter-Telefonie-Lösung benötigt, die standortübergreifend / ortsunabhängig verfügbar ist, die alle wesentliche Dienst-Merkmale für Callcenter und eine einheitliche Rufnummer zur Erreichbarkeit bietet.

2 Innerorganisatorische Ansprechpartner[2]

Verantwortliche Fachabteilung	IT-Services
Fachlicher Ansprechpartner	Frau Fatma Mutlu
Telefon	02371 – 566 2646
E-Mail-Adresse	mutlu.fatma@fh-swf.de
Technischer Ansprechpartner	Frau Fatma Mutlu
Telefon	02371 – 566 2646
E-Mail-Adresse	mutlu.fatma@fh-swf.de

3 Angaben zum ggf. mit dem Verantwortlichen gemeinsam Verantwortlichen[1]

Name

Straße

* [1,2] Hinweis: Bei Angaben, die im Folgenden mit ([1]) gekennzeichnet sind, handelt es sich um solche, die gemäß Art. 30 DS-GVO zwingender Bestandteil des VVT sein müssen. Angaben, die im Folgenden mit ([2]) gekennzeichnet sind, sind solche, die aus Gründen der Rechenschaftspflicht gemäß Art. 5 Abs. 2 DS-GVO notwendig sind. Weitere Informationen dazu finden Sie in unseren Ausfüllhinweisen.

PLZ, Ort _____

Land _____

Telefon _____

E-Mail-Adresse _____

4 Beschreibung der Verarbeitungstätigkeit[2]

Dieser Dienst ermöglicht es, ohne eine Hardware-Telefonanlage, die speziellen notwendigen Funktionen solch einer Callcenter-Telefonanlage (z.B. Warteschleife, Sprachansagen, Sprachspeicher, Einklinken von Call-Center-Mitarbeitern, Konferenzfunktion, Makeln, etc.) im Netzwerk mit passenden Endgeräten zu nutzen.

5 Kategorien personenbezogener Daten[1]

In der Spalte Bes. ist ein „x“ zu setzen, wenn das jeweilige Datum einer besonderen Kategorie personenbezogener Daten gemäß Art. 9 DS-GVO oder Art. 10 DS-GVO zuzuordnen ist.

Lfd. Nr	Beschreibung	Bes.
1	Daten die vom Kunden telefonisch übermittelt werden: Störmeldungen bzw. Supportanfragen: Beschreibung des Anliegens (i.d.R. Problembeschreibungen) Benutzerdaten (Beschäftigte) bestehend aus - Name, Vorname, Mail-Account - E-Mail-Adresse, Rufnummer, Faxnummer - Beschäftigungsstelle - Adresse Benutzerdaten (Studierende) bestehend aus - Name, Vorname, Mail-Account - E-Mail-Adresse - Matrikelnummer - Adresse	
2	Daten die vom 1st bzw. 2nd Level Support telefonisch übermittelt werden: Lösungsvorschläge / Problemlösung	
3	Daten die systemtechnisch erzeugt werden: Zeitstempel: Zeitpunkt des Anrufs (Tag und Uhrzeit) Username des IT-Servicedesk Mitarbeiters Status des Anrufs: beendeter Anruf, unbeantworteter Anruf, zurückgewiesener Anruf Telefonnummer des Anrufers Wartezeit des Anrufers Gesprächszeit (Dauer des Anrufes) / Klingelzeit Sprachnachricht	

Hinweis: Erfolgt eine umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten oder von personenbezogenen Daten über strafrechtliche

Verurteilungen und Straftaten, so ist eine Datenschutz-Folgenabschätzung (siehe Ziffer 13) durchzuführen.

6 Kategorien betroffener Personen[1]

Lfd. Nr. aus 5.	Betroffene
1 – 2	Angehörige der Hochschule (Beschäftigte und Studierende)
1 – 3	Angehörige der IT-Services

7 Rechtsgrundlage der Verarbeitungstätigkeit[2]

Lfd. Nr. aus 5.	Bezeichnung der Vorschrift(en) oder Hinweis auf **Einwilligung** (Einwilligungstext bitte als Anhang beifügen)	Erläuterungen
1 - 3	Art. 6 Abs. 1 Satz 1 lit. e) DSGVO i.V.m. § 3 Abs. 1 DSG NRW und Dienstvereinbarung für den Betrieb eines IT-Servicedesks an der FH SWF	

8 Empfänger personenbezogener Daten[1]

8.1 Interne Empfänger innerhalb der Organisation des Verantwortlichen

Lfd. Nr. aus 5.	Interne Stelle	Zweck
1 – 3	IT-Servicedesk MA	Anfragenbearbeitung
1 – 3	IT-Services MA (SG 6.1 – 6.4)	Anfragenbearbeitung

8.2 Externe Empfänger

In der Spalte ADV ist ein „x“ zu setzen, wenn der Empfänger im Rahmen einer Auftragsverarbeitung tätig wird. Dann ist beim Zweck der Tätigkeitsumfang zu beschreiben.

Lfd. Nr. aus 5.	Empfänger, i.d.R. mit ladungsfähiger Anschrift	Zweck bzw. Tätigkeit	ADV

Sofern Empfänger ihren Sitz in einem Drittland haben oder es sich um eine internationale Organisation handelt:

Empfänger aus 8.2. mit Bezeichnung des Drittlandes	Die Weitergabe wird gestützt auf
	☐ einen Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DS-GVO), ☐ die Herstellung eines ausreichenden Datenschutzniveaus durch verbindliche interne Datenschutzvorschriften (Art. 46 Abs. 2 lit. b i.V.m. 47 DS-GVO, ☐ die Herstellung eines ausreichenden Datenschutzniveaus durch Standarddatenschutzklauseln (Art. 46 Abs. 2 litt. c und d DS-GVO, ☐ die Herstellung eines ausreichenden Datenschutzniveaus durch genehmigte Verhaltensregeln (Art. 46 Abs. 2 lit. e i.V.m.

	40 DS-GVO, ☐ die Herstellung eines ausreichenden Datenschutzniveaus durch ein Zertifizierungsmechanismus (Art. 46 Abs. 2 lit. f i.V.m. 42 DS-GVO), ☐ die Herstellung eines ausreichenden Datenschutzniveaus durch folgende sonstige Maßnahmen (Art. 46 Abs. 2 lit. a, Abs. 3 litt. a und b DS-GVO): ☐ folgenden Ausnahmetatbestand des Art. 49 DS-GVO:

9 Zugriffsberechtigte Personengruppen oder Personen, die allein zugriffsberechtigt sind[2]

Lfd. Nr. aus 5.	Personen(gruppe)	Umfang
1 – 3	IT-Servicedesk MA 1st Level	Anfragenbearbeitung
1 – 3	IT-Services MA 2nd Level	Anfragenbearbeitung

10 Fristen für die Löschung[1]

Lfd. Nr. aus 5.	Frist

11 Allgemeine Beschreibung der eingesetzten Hardware, Software und der Vernetzung[2]

11.1 Eingesetzte Software auf Klienten und Servern außer dem Betriebssystem

Lfd. Nr.	Art der Software	Bezeichnung	Version	Einsatz
	wird von NFON betrieben			☐ Klient ☐ Server

11.2 Beteiligte Klienten (Arbeitsplatzrechner, mobile Rechner, Terminal, Videokamera usw.)

☒ Es handelt sich um eine Webanwendung, bei der die Klienten nicht näher bestimmbar sind

Anzahl	Typ	Betriebssystem, Version	Software, lfd. Nr. aus 11.1	Netzwerk & Hardware	Daten, lfd, Nr. aus 5.
				☐ IPv4 ☐ IPv6 ☐ SSD-Festplatte ☐ Ext. Medium	

11.3 Beteiligte Server

Lfd. Nr.	Funktion	Betriebssystem, Version, Virtualisierung	Software, lfd. Nr. aus 11.1	Hardware	Standort	Daten, lfd. Nr. aus 5.
	wird von NFON betrieben	☐ virtualisiert		☐ SSD-Festplatte	Ort/Firma: ☐ extern ☐ intern	

11.4 Datensicherung

Lfd. Nr.	Medium	Server, lfd. Nr. aus 11.3	Software, lfd. Nr. aus 11.1	Aufbewahrungsort	Daten, lfd. Nr. aus 5.
	wird von NFON betrieben				

11.5 Darstellung der Netzstruktur

☒ Ist als folgende Anlage beigefügt: Anlage 1

11.6 Verwendete Protokolle, Dienste und Verschlüsselung

Übertragungsabschnitt	Software, lfd. Nr. aus 11.1	Protokoll, Port	Verschlüsselung
Wissenschaftsnetz X-Win Rechenzentren in Nürnberg und München		SIP-Trunk	TLS/SRTP Verschlüsselung

12 Technische und organisatorische Maßnahmen[1]

☒ Es wird auf folgendes Dokument verwiesen:

NFON Technische und organisatorische Maßnahmen nach Art. 32 Abs. 1 lit. B DSGVO

☐ Es sind (ggf. zusätzlich) folgende Maßnahmen getroffen:

12.1 Pseudonymisierung

Siehe NFON Technische und organisatorische Maßnahmen nach Art. 32 Abs. 1 lit. B DSGVO

12.2 Verschlüsselung

Siehe NFON Technische und organisatorische Maßnahmen nach Art. 32 Abs. 1 lit. B DSGVO

12.3 Gewährleistung der Vertraulichkeit

Siehe NFON Technische und organisatorische Maßnahmen nach Art. 32 Abs. 1 lit. B DSGVO

12.4 Gewährleistung der Integrität

Siehe NFON Technische und organisatorische Maßnahmen nach Art. 32 Abs. 1 lit. B DSGVO

12.5 Gewährleistung der Verfügbarkeit

Siehe NFON Technische und organisatorische Maßnahmen nach Art. 32 Abs. 1 lit. B DSGVO

12.6 Gewährleistung der Belastbarkeit der Systeme

Siehe NFON Technische und organisatorische Maßnahmen nach Art. 32 Abs. 1 lit. B DSGVO

12.7 Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall

Siehe NFON Technische und organisatorische Maßnahmen nach Art. 32 Abs. 1 lit. B DSGVO

12.8 Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der

Siehe NFON Technische und organisatorische Maßnahmen nach Art. 32 Abs. 1 lit. B DSGVO

12.9 Weitere Maßnahmen:

☐ Sensibilisierung und/oder Schulung der an Verarbeitungsvorgängen Beteiligten
☐ Beteiligung des/der zuständigen Datenschutzbeauftragten
☐ Hinweis/Verpflichtung der an Verarbeitungsvorgängen Beteiligten auf das Datengeheimnis
☐ Folgende Maßnahmen, die die nachträgliche Überprüfung und Feststellung gewährleisten, ob und von wem personenbezogene Daten erfasst, verändert oder gelöscht worden sind:
☐ Im Falle einer Übermittlung oder Zweckänderung:
Folgende spezifischen Verfahrensregelungen werden getroffen, um die Einhaltung des LDSG und der DS-GVO sicherzustellen:

☐ Sonstiges:

12.10 Weitere Dokumente:

☐ Interne Verhaltensregeln
☐ Risikoanalyse
☐ Allgemeine Datensicherheitsbeschreibung
☐ Umfassendes Datensicherheitskonzept
☐ Wiederanlaufkonzept
☐ Zertifikat: ISO 27001, ITIL, eco Datencenter Five Star
Zertifizierungsstelle: siehe NFON Technische und organisatorische Maßnahmen nach Art. 32 Abs. 1 lit. B DSGVO
☐ Sonstiges:

13 Datenschutz-Folgenabschätzung[2]

☐ Eine Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO ist notwendig (insbesondere immer notwendig, wenn eine umfangreiche Verarbeitung besonderer Kategorien personenbezogener Daten erfolgt).

☒ Eine Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO ist nicht notwendig.

Verzeichnis von Verarbeitungstätigkeiten

des Verantwortlichen gemäß Art. 30 Abs. 1 DS-GVO

- Besonderer Teil * -

Datum _____

Az. (intern)

☒ Neue Verarbeitungstätigkeit

☐ Änderung bestehender Verarbeitungstätigkeit

1 Bezeichnung der Verarbeitungstätigkeit[1]

Bezeichnung der Verarbeitungstätigkeit	IT-Servicedesk Fernwartungssoftware FastViewer
Zweck der Verarbeitung	Zur Verfügung stellen eines sicheren Netzinternen Remote Services

2 Innerorganisatorische Ansprechpartner[2]

Verantwortliche Fachabteilung	IT-Services
Fachlicher Ansprechpartner	Frau Fatma Mutlu
Telefon	02371 – 566 2646
E-Mail-Adresse	mutlu.fatma@fh-swf.de
Technischer Ansprechpartner	Frau Fatma Mutlu
Telefon	02371 – 566 2646
E-Mail-Adresse	mutlu.fatma@fh-swf.de

3 Angaben zum ggf. mit dem Verantwortlichen gemeinsam Verantwortlichen[1]

Name _____

Straße _____

PLZ, Ort _____

_____

* [1,2] Hinweis: Bei Angaben, die im Folgenden mit ([1]) gekennzeichnet sind, handelt es sich um solche, die gemäß Art. 30 DS-GVO zwingender Bestandteil des VVT sein müssen. Angaben, die im Folgenden mit ([2]) gekennzeichnet sind, sind solche, die aus Gründen der Rechenschaftspflicht gemäß Art. 5 Abs. 2 DS-GVO notwendig sind. Weitere Informationen dazu finden Sie in unseren Ausfüllhinweisen.

Land

Telefon

E-Mail-Adresse

4 Beschreibung der Verarbeitungstätigkeit[2]

Zur Fernbetreuung bei PC-Problemen wird eine Fernwartungssoftware eingeführt. Durch die Einführung der neuen Software soll den IT-Mitarbeiterinnen und IT-Mitarbeitern, die IT-Anwenderinnen und IT-Anwender betreuen, ein Arbeitsmittel zur Verfügung gestellt werden, um bei Bedarf Betreuung mittels Fernwartung leisten zu können.

So kann die IT-Mitarbeiterin oder der IT-Mitarbeiter mit dieser Software:

- eine Übersicht über die Hardwarekomponenten und die aktive Software erhalten,

- den Bildschirm angezeigt bekommen,

- Software auf dem Rechner installieren oder deinstallieren,

- Eingriffe in Dateien vornehmen,

- steuernd in den Dialog eingreifen,

- den gesteuerten Rechner neu starten,

- die Bedienung kontrolliert übernehmen.

5 Kategorien personenbezogener Daten[1]

In der Spalte Bes. ist ein „x“ zu setzen, wenn das jeweilige Datum einer besonderen Kategorie personenbezogener Daten gemäß Art. 9 DS-GVO oder Art. 10 DS-GVO zuzuordnen ist.

Lfd. Nr	Beschreibung	Bes.
1	Daten die systemtechnisch übermittelt werden: - Benutzerkennung	
2	Daten die systemtechnisch erzeugt werden: - Datum (Dauer – Zeitstempel „von“ „bis“) - IP-Adresse - Sitzungsnummer - Technisches Protokoll der Sitzung	
3	Daten die vom Kunden an die IT-Servicedesk MA übermittelt werden: Störmeldungen bzw. Supportanfragen: Beschreibung des Anliegens (i.d.R. Problembeschreibungen)	

Hinweis: Erfolgt eine umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten, so ist eine Datenschutz-Folgenabschätzung (siehe Ziffer 13) durchzuführen.

6 Kategorien betroffener Personen[1]

Lfd. Nr. aus 5.	Betroffene
3	Angehörige der Hochschule (Beschäftigte und Studierende)
1, 3	Angehörige der IT-Services
1, 2	Administratoren von FastViewer (TU Dortmund)

7 Rechtsgrundlage der Verarbeitungstätigkeit[2]

Lfd. Nr. aus 5.	Bezeichnung der Vorschrift(en) oder Hinweis auf **Einwilligung** (Einwilligungstext bitte als Anhang beifügen)	Erläuterungen
1, 2, 3	Art. 6 Abs. 1 Satz 1 lit. e) DSGVO i.V.m. § 3 Abs. 1 DSG NRW und Dienstvereinbarung für den Betrieb eines IT-Servicedesks an der FH SWF	Anlage 1

8 Empfänger personenbezogener Daten[1]

8.1 Interne Empfänger innerhalb der Organisation des Verantwortlichen

Lfd. Nr. aus 5.	Interne Stelle	Zweck
1	Registrierte Nutzer des Fernwartungstools (IT-Services MA)	
1, 2	Administratoren	

8.2 Externe Empfänger

In der Spalte ADV ist ein „x“ zu setzen, wenn der Empfänger im Rahmen einer Auftragsverarbeitung tätig wird. Dann ist beim Zweck der Tätigkeitsumfang zu beschreiben.

Lfd. Nr. aus 5.	Empfänger, i.d.R. mit ladungsfähiger Anschrift	Zweck bzw. Tätigkeit	ADV

Sofern Empfänger ihren Sitz in einem Drittland haben oder es sich um eine internationale Organisation handelt:

Empfänger aus 8.2. mit Bezeichnung des Drittlandes	Die Weitergabe wird gestützt auf
	☐ einen Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DS-GVO), ☐ die Herstellung eines ausreichenden Datenschutzniveaus durch verbindliche interne Datenschutzvorschriften (Art. 46 Abs. 2 lit. b i.V.m. 47 DS-GVO, ☐ die Herstellung eines ausreichenden Datenschutzniveaus durch Standarddatenschutzklauseln (Art. 46 Abs. 2 litt. c und d DS-GVO, ☒ die Herstellung eines ausreichenden Datenschutzniveaus durch genehmigte Verhaltensregeln (Art. 46 Abs. 2 lit. e i.V.m. 40 DS-GVO,

	☐ die Herstellung eines ausreichenden Datenschutzniveaus durch ein Zertifizierungsmechanismus (Art. 46 Abs. 2 lit. f i.V.m. 42 DS-GVO), ☐ die Herstellung eines ausreichenden Datenschutzniveaus durch folgende sonstige Maßnahmen (Art. 46 Abs. 2 lit. a, Abs. 3 litt. a und b DS-GVO): ☐ folgenden Ausnahmetatbestand des Art. 49 DS-GVO:

9 Zugriffsberechtigte Personengruppen oder Personen, die allein zugriffsberechtigt sind[2]

Lfd. Nr. aus 5.	**Personen(gruppe)**	**Umfang**
1, 2	Administratoren von FastViewer (Ausgewählter Personenkreis TU Dortmund)	
3	„2nd – Level“ Support (Mitarbeiter im operativen Tätigkeitsfeld des IT-Services)	
3	„1st – Level“ Support (Ausgewählter Personenkreis IT-Servicedesk)	

10 Fristen für die Löschung[1]

Lfd. Nr. aus 5.	**Frist**

11 Allgemeine Beschreibung der eingesetzten Hardware, Software und der Vernetzung[2]

11.1 Eingesetzte Software auf Klienten und Servern außer dem Betriebssystem

Lfd. Nr.	Art der Software	Bezeichnung	Version	Einsatz
1	Kompiliertes EXE File mit allen Modulen intern	FastViewer.exe	Lfd. aktualisiert	☒ Klient ☐ Server
2	Servermodul	FV Server	Lfd. aktualisiert	☐ Klient ☒ Server

11.2 Beteiligte Klienten (Arbeitsplatzrechner, mobile Rechner, Terminal, Videokamera usw.)

☒ Es handelt sich um eine Webanwendung, bei der die Klienten nicht näher bestimmbar sind

Anzahl	Typ	Betriebssystem, Version	Software, lfd. Nr. aus 11.1	Netzwerk & Hardware	Daten, lfd, Nr. aus 5.
				☐ IPv4 ☐ IPv6 ☐ SSD-Festplatte ☐ Ext. Medium	

11.3 Beteiligte Server

Lfd. Nr.	Funktion	Betriebssystem, Version, Virtualisierung	Software, lfd. Nr. aus 11.1	Hardware	Standort	Daten, lfd. Nr. aus 5.
1	verschlüsselte Kommunikation	☒ virtualisiert	2	☒ SSD-Festplatte	Ort/Firma: ☒ extern ☐ intern	

11.4 Datensicherung

Lfd. Nr.	Medium	Server, lfd. Nr. aus 11.3	Software, lfd. Nr. aus 11.1	Aufbewahrungsort	Daten, lfd. Nr. aus 5.
1	Platten Cluster	1	2	TU Dortmund	

11.5 Darstellung der Netzstruktur

☒ Ist als folgende Anlage beigefügt: Anlage_2_FastViewer.pdf

11.6 Verwendete Protokolle, Dienste und Verschlüsselung

Übertragungsabschnitt	Software, lfd. Nr. aus 11.1	Protokoll, Port	Verschlüsselung
Eigenes Protokoll	1, 2	TCP 80, 443, 5000	256 Bit AES (TÜV Zertifikat, OPDV und FIDUCIA jährlich aktuell)

12 Technische und organisatorische Maßnahmen[1]

☒ Es wird auf folgendes Dokument verwiesen: Anlage 3

☐ Es sind (ggf. zusätzlich) folgende Maßnahmen getroffen:

12.1 Pseudonymisierung

Nur sichtbar für benannte Admins

12.2 Verschlüsselung

256 Bit AES
(TÜV Zertifikat, OPDV und FIDUCIA jährlich aktuell)

12.3 Gewährleistung der Vertraulichkeit

Zugang zum Server nur über zertifizierte Rechner

12.4 Gewährleistung der Integrität

Alle 2 Wochen durchgeführter Pen Test

12.5 Gewährleistung der Verfügbarkeit

SnapShot der VM steht bei Ausfall nach 60 Minuten zur Verfügung

12.6 Gewährleistung der Belastbarkeit der Systeme

Vierteljähriger Test auf Last und permanente Kontrolle

12.7 Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall

SnapShot der VM, Sicherung über Veeam in der VM

12.8 Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

Siehe 12.4 und 12.6

12.9 Weitere Maßnahmen:

☒ Sensibilisierung und/oder Schulung der an Verarbeitungsvorgängen Beteiligten
☒ Beteiligung des/der zuständigen Datenschutzbeauftragten
☒ Hinweis/Verpflichtung der an Verarbeitungsvorgängen Beteiligten auf das Datengeheimnis
☒ Folgende Maßnahmen, die die nachträgliche Überprüfung und Feststellung gewährleisten, ob und von wem personenbezogene Daten erfasst, verändert oder gelöscht worden sind:
☐ Im Falle einer Übermittlung oder Zweckänderung:
Folgende spezifischen Verfahrensregelungen werden getroffen, um die Einhaltung des LDSG und der DS-GVO sicherzustellen:

☐ Sonstiges:

12.10 Weitere Dokumente:

☐ Interne Verhaltensregeln
☐ Risikoanalyse
☐ Allgemeine Datensicherheitsbeschreibung
☐ Umfassendes Datensicherheitskonzept

☐ Wiederanlaufkonzept
☐ Zertifikat:
Zertifizierungsstelle:
☐ Sonstiges:

13 Datenschutz-Folgenabschätzung[2]

☐ Eine Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO ist notwendig (insbesondere immer notwendig, wenn eine umfangreiche Verarbeitung besonderer Kategorien personenbezogener Daten erfolgt).

☒ Eine Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO ist nicht notwendig.