

|  |
| --- |
| **Verzeichnis von Verarbeitungstätigkeiten Verantwortlicher****gem. Artikel 30 Abs. 1 DS-GVO** |
| **Angaben zum Verantwortlichen im Sinne der DS-GVO¹**Name Universität Rostock, gesetzlich vertreten durch den RektorStraße Universitätsplatz 1Postleitzahl 18055Ort RostockTelefon 0381 498 1000E-Mail-Adresse rektor@uni-rostock.deInternet-Adresse https://www.uni-rostock.de/ |
| **Angaben zur datenverarbeitenden Stelle/inhaltlich verantwortlichen Struktureinheit**Bezeichnung      Ansprechpartner\*in      Straße      Postleitzahl, Ort      Telefon      E-Mail-Adresse       |
| **Angaben zur technisch verantwortlichen Fachabteilung/Struktureinheit**Bezeichnung  IT-und Medienzentrum der UR   Ansprechpartner\*in  Kerstin Baier    Straße  Albert-Einstein-Str. 22    Postleitzahl, Ort  18055 Rostock    Telefon  0381 4985335    E-Mail-Adresse evasys.admin@uni-rostock.de |
| **Angaben zur Person der/des Datenschutzbeauftragten** Anrede Frau Titel Dr.    Name, Vorname Fröhlich, KatjaStraße Albert-Einstein-Str. 22 (Konrad-Zuse-Haus), Raum 104Postleitzahl 18055Ort RostockTelefon 0381 498 8333 E-Mail-Adresse datenschutzbeauftragte@uni-rostock.de |

|  |
| --- |
| Bezeichnung des Verfahrens: |
| Datum der Einführung:       | Datum der letzten Änderung:       |
| Beschreibung der Verarbeitungstätigkeit³  | **Vorhaben** Im Rahmen der… [Befragenden benennen, ggf. übergeordneten Kontext der Befragung benennen] soll eine Befragung zur [Thema der Befragung einfügen] durchgeführt werden. Die Befragung erfolgt ausschließlich elektronisch mittels der durch die UR bereitgestellten und gehosteten Software EvaSyS. Die Speicherung sämtlicher Daten findet ausschließlich auf universitätsinternen Servern statt. Eine (zusätzliche) Speicherung auf lokalen Dienstrechnern und/oder privaten Endgeräten und/oder Speichermedien erfolgt nicht.Eine Zwischenspeicherung der erhobenen Daten erfolgt auf dem Server der UR in einem Netzlaufwerk-Ordner. Der Zugang zu diesen Daten wird durch Zugangsberechtigungen geregelt. Zugriff haben nur Personen, die am… [datenverarbeitende Stelle und ggf. Dritte benennen] tätig sind. Die Befragung soll am [Startdatum eintragen] starten und am [Enddatum eintragen] beendet werden. Die Befragungsdaten werden nach Beendigung der Auswertung gelöscht, spätestens aber am [Zeitpunkt der Löschung eintragen].**Anmeldevorgang**Die potentiellen Befragungsteilnehmer erhalten per E-Mail eine Einladung zu dieser Befragung. Die E-Mailadressen der Einrichtungen wurden durch … [Stelle benennen] zur Verfügung gestellt. Die E-Mail enthält [ ]  eine automatisch generierte TAN [ ]  einen Linkfür den Zugang zur Befragungssoftware EvaSyS.**Einwilligung zur Teilnahme**Die potentiellen Teilnehmer werden auf der Startseite der Befragung über das Ziel der Studie sowie die Einhaltung der Datenschutzvorgaben informiert. Ihre Einwilligung wird eingeholt, indem eine Einverständnis-Box angeklickt werden muss als Voraussetzung, dass die Seite mit der eigentlichen Befragung erscheint. Die Teilnehmer haben, sowohl auf dieser als auch auf der nächsten Seite die Möglichkeit zum jederzeitigen Abbruch der Befragung. **Auswertung und Ergebnisdarstellung**Die Ergebnisse werden mitEvaSys für die Auswertung und Darstellung der Daten in [Software benennen, mit der gearbeitet wird, bspw. Excel] aufbereitet. Die zu erstellende Publikation wird Daten in aggregierter Form aufgreifen, aus denen jedoch keine Rückschlüsse auf die einzelnen Teilnehmer möglich sind. In die Auswertung einbezogen wird lediglich…. |
| Zweck der Verarbeitung |  |
| Datenflussdiagramm4 |                          |
| Name des eingesetzten Verfahrens (Software, IT-System, Tool, Dienst o.ä. technische Unterstützung) | Die elektronische Befragung wird mittels der on-premise-Lösung EvaSys (von Electric Paper Evaluationssysteme GmbH) durchgeführt. Die Auswertung der erhobenen Daten erfolgt mittels [Software benennen, mit der gearbeitet wird, bspw. Microsoft Office (Word und/oder Excel), SPSS]. |
| Grundlage der Datenverarbeitung | [x]  Rechtsnorm  [ ]  inneruniversitär (bitte genaue Angabe von Paragraph, Absatz, Satz, Alt. etc.) [x]  Bundes-/Landesrecht (bitte genaue Angabe von Paragraph, Absatz, Satz, Alt. etc.)Art. 6 Abs. 1 S. 1 lit. a) DS-GVO [x]  Einwilligung der von der Datenverarbeitung betroffenen Personen (bitte beifügen) |

**1. Kategorien personenbezogener Daten und Zweck der Datenverarbeitung5**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lfd. Nr** | **Kategorie** | **Beschreibung** | **Zweck der Verarbeitung** |
| 1 | Kontaktdaten | E-Mail-Adresse der potentiellen Umfrageteilnehmer | Kontaktaufnahme zwecks Befragung |
| 2 | Daten, die durch/bei Nutzung von EvaSyS anfallen | IP-Adresse, Protokolldaten etc.; Einzelheiten s. Anhang 1 | Nutzung der Befragungssoftware |
| 3 | Inhaltsdaten | Inhalte der Fragebögen, Einzelheiten s. Anhang 2 |  |
| 4 |  |  |  |
| 5 |  |  |  |

**2. Kategorien betroffener Personen**

|  |  |
| --- | --- |
| **Datenkategorie (Lfd. Nr.** **aus 1.)** | **Betroffene** |
| 1-3 | Umfrageteilnehmer |
| 2 | Personen, die Umfrage durchführen |
|  |  |
|  |  |
|  |  |

**3. Empfänger personenbezogener Daten7**

3.1 Interne Empfänger innerhalb der Universität

|  |  |  |
| --- | --- | --- |
| **Datenkategorie (Lfd. Nr. aus 1.)** | **Interne Stelle** | **Zweck** |
| 1-3 | ITMZ, Admin EvaSyS | Administration der Software |
| 1, 3 | Personen, die Umfrage durchführen | Durchführung der Umfrage |
|  |  |  |
|  |  |  |
|  |  |  |

3.2 Externe Empfänger

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

|  |  |  |  |
| --- | --- | --- | --- |
| **Datenkategorie (Lfd. Nr. aus 1.)** | **Empfänger** | **Zweck bzw. Tätigkeit** | **AVV** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

3.3 Übermittlung von personenbezogenen Daten an ein Drittland oder einer internationalen Organisation

[ ]  Eine Datenübermittlung findet nicht statt und ist auch nicht geplant

[ ]  Eine Datenübermittlung findet statt:

[ ]  an folgendes Drittland/folgende Drittländer:

[ ]  an folgende internationale Organisation/en:

**4. Löschkonzept8**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Datenkategorie (Lfd. Nr. aus 1.)** | **Löschfrist** | **Startzeitpunkt der Löschfrist** | **Umsetzungsregel** | **Verantwortliche/r** |
| 1 – Kontaktdaten |  | Absenden der E-Mail, die Einladung zur Teilnahme an Umfrage enthält  | manuelle Löschung durch [Person benennen, die löschen soll; Funktionsbezeichnung genügt] | Personen, die Umfrage durchführen |
| 2 – IP-Adresse des jew. Teilnehmers | unmittelbar nach Ablauf der Session | Beginn der Session | Automatische Löschung durch EvaSyS | Admin EvaSyS |
| 2 - Protokolldaten | 12 Monate nach Ablauf der Befragung | Beginn der Befragung | Automatische Löschung durch EvaSyS | AdMin EvaSyS |
| 3 – Inhaltsdaten |  |  |  |  |
| 4 |  |  |  |  |
| 5 |  |  |  |  |
|  |  |  |  |  |

**5. Berechtigungskonzept (Rechte- und Rollenkonzept)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Datenkategorie (Lfd. Nr. aus 1.)** | **Empfängerkategorie (Lfd. Nr. aus 2.)** | **Rechte** | **Pflichten** | **Beschreibung Verfahren zur Vergabe und zum Entzug von Berechtigungen** |
| 1-Kontaktdaten | Teilbereichs-Admin evasys | Einsehen der Kontaktdaten (nur, sofern Lehrveranstaltung angelegt wird) |  |  |
| 1-Kontaktdaten | Personen, die Umfrage durchführen | Starten der Umfrage | Löschen, sobald die Kontaktdaten nicht mehr benötigt werden |  |
| 2 - Daten, die bei/durch Nutzung von evasys anfallen (IP-Adresse der Umfrageteilnehmer und Protokolldaten)  | ITMZ-Admin evasysTeilbereichsadmin EvaSys | Einsicht in Zustellungen, Logbuch und Protokolle (Lösch-, Webservice- und Mailservice-Protokolle) | ITMZ-Admin evasys:- Updates einspielen- Kommunikation mit dem Hersteller (bspw. wenn Fehler in der Software auftreten)- technische Unterstützung der AnwenderTeilbereichsadmin: | Admin evasys: Rechte und Pflichten wurden von Leitung ITMZ und Abteilungsleiter mündlich an Admin evasys übertragenTeilbereichsadmin: Admin ITMZ erteilt Rechte, Kriterium ist Anforderung desjenigen, der evasys nutzen möchte |
| 3-Inhaltsdaten |  ITMZ Admin evasys und Teilbereichsadmin evasys | Zugriff auf alle Teilbereiche (Löschen, Hinzufügen, Bearbeiten) bzw. (bei Teilsbereichsadmin: auf den zugewiesenen Teilbereich)Erstellen von UmfragenEinsicht in zentral generierte Umfrageergebnisse eines oder mehrerer (Teil)BereicheEinsicht in aktivierte Nutzerkonten, deren Umfragen und ErgebnisseArchivieren von Rohdaten aus UmfragenLöschen und/oder Kategorisieren von Antworten auf offene FragenKonfigurieren der Software nach individuellen Wünschen (bspw. Vergabe von Einsichtsrechten in Qualitätsübersichten, Einrichten von Benachrichtigungen über auffällige Ergebnisse des Qualitätsmanagements)Zugriff auf Reportverwaltung, Textvorlagen, OnlinetemplatesSenden von E-Mails an Support | ITMZ-Admin evasys:- Updates einspielen- Kommunikation mit dem Hersteller (bspw. wenn Fehler in der Software auftreten)- technische Unterstützung der AnwenderTeilbereichsadmin: | Rechte und Pflichten wurden von Leitung ITMZ und Abteilungsleiter mündlich übertragen  Teilbereichsadmin: Admin ITMZ erteilt Rechte, Kriterium ist Anforderung desjenigen, der evasys nutzen möchte |
| 3-Inhaltsdaten | Personen, die Umfrage durchführen | Erstellen von UmfragenZugriff auf die eigenen erstellten Umfragen (inkl. Textvorlagen) und deren Ergebnisse sofern durch ITMZ-Admin EvaSyS zugelassen, auch Zugriff auf die den Durchführenden der Umfrage betreffenden Umfrageergebnisse zentraler Evaluationen |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**6. Technische und organisatorische Maßnahmen**

[x]  Es wird auf folgende Dokumente verwiesen:

|  |
| --- |
| IT-Sicherheitsleitlinie der Universität Rostock |
| IT-Sicherheitskonzept des IT- und Medienzentrums der Universität Rostock |
| Nutzungsordnung des IT- und Medienzentrums |
| Betriebsregelung und Benutzungsordnung für das Datenkommunikationsnetz der Universität Rostock RUN |

[ ]  Es sind (ggf. zusätzlich) folgende Maßnahmen getroffen:

|  |
| --- |
| 5.1 Pseudonymisierung      |
| 5.2 Verschlüsselung      |
| 5.3 Gewährleistung der Vertraulichkeit      |
| 5.4 Gewährleistung der Integrität      |
| 5.5 Gewährleistung der Verfügbarkeit      |
| 5.6 Gewährleistung der Belastbarkeit der Systeme      |
| 5.7 Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall      |
| 5.8 Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen      |
| 5.9 Weitere Maßnahmen:[ ]  Beteiligung der Datenschutzbeauftragten Stellungnahme des DSB erfolgte am:      [ ]  Beteiligung des IT-Sicherheitsbeauftragten Stellungnahme des DSB erfolgte am:      [ ]  Sonstiges:       |

**Anlage 1** – Daten, die in Zusammenhang mit der Nutzung von evasys verarbeitet werden

Meldet sich ein evasys-Anwender erfolgreich an, wird dessen aktuelle IP-Adresse in der Datenbank den Anwenderdaten zugewiesen. Die Information verbleibt in der Datenbank und wird bei der nächsten Anmeldung in evasys überschrieben.

Weiterhin wird nach erfolgreicher Anmeldung die IP-Adresse des angemeldeten Nutzers in der PHP-Session gespeichert, sofern die Option „Beschränkter Zugriff“ (evasys Konfiguration > Systemsicherheit) in evasys aktiviert ist. Die Session wird in einer Datei auf dem Server gespeichert und nach Ablauf gelöscht.

Schlägt ein Anmeldeversuch eines evasys-Anwenders fehl, wird dessen IP-Adresse in der Datenbank als Login-Versuch gespeichert und es werden die Anmeldeversuche für die IP-Adresse gezählt, um nach dem dritten erfolglosen Versuch ein Captcha anzuzeigen. Für mindestens 15 Minuten werden die Daten in der Datenbank vorgehalten. Ruft jemand nach mindestens 15 Minuten die evasys Login-Seite auf, werden die Einträge in der Datenbank gelöscht.

Weiterhin werden IP-Adresse des evasys-Servers und IP-Adresse der Scanstation im Rahmen der Aktivierung abgeglichen. Diese IP-Adressen sind keinen Personen zuzuordnen. Außerhalb von evasys speichert der Webserver die IP-Adresse einer jeden http-Anfrage in einer Datei. Dies trifft auch bei Requests durch Onlineumfragenteilnehmer zu.

Im Zustellungsprotokoll (nur für den Admin einsehbar) wird vermerkt, wer wann zu welcher Umfrage eine Mail erhalten hat. Es wird auch angezeigt, wenn eine Zustellung nicht möglich war. Für den Ersteller der Befragung sind in der Datendatei nur die Rückantworten sichtbar.

Protokolliert werden folgende Löschvorgänge:

* Teilbereiche
* Nutzer
* Lehrveranstaltungen/Themen
* Umfragen
* TANs
* Fragebögen
* Ordner (bei aktiven Dozenten

Zu jedem Löschvorgang wird protokolliert:

* Nutzer/in: Wer hat gelöscht?
* Objekttyp und Beschreibung: Was wurde gelöscht?
* Datum: Wann wurde gelöscht?
* ID des auslösenden Vorgangs: Durch welchen anderen Löschvorgang wurde diese Löschung ausgelöst?

Das ITMZ der UR hat folgende Sicherheitsmaßnahmen aktiviert:

* Zugriff des Umfrageerstellers kann nur aus dem Uni-Netz erfolgen
* Beim Erstellen von TAN basierten Umfragen erhält jeder Teilnehmer eine andere TAN/Link und kann nur einmal an der Umfrage teilnehmen
* Zum Versenden werden die Mailadressen benutzt
* Die Teilnehmer der Umfrage kennen die anderen teilnehmenden Personen nicht.
* Folgende Einstellungen sind im System hinterlegt:





**Die evasys-Datenbank enthält:**

* die gesamten Profildaten (Organisation, Teilbereiche, Nutzer)
* sämtliche Umfragen mit Rohdaten sowie statistischen Kennwerten
* den Inhalt sowie die Auswertungsregeln aller Fragebögen
* Betriebsdaten (Logbücher, Erhebungsperioden, TAN-Listen)
* Die Datenbankzugangsdaten sind verschlüsselt, so dass auch der Systembetreuer nicht auf die Erhebungsdaten zugreifen kann.

**Automatische Updateüberprüfung**

Nach dem Login des Administrators wird in regelmäßigen Abständen (Standardwert 30 Tage) eine automatische Überprüfung auf Updates durchgeführt. Bei den Updateprüfungen werden Daten über das evasys-System vom Browser des Administrators an den Updateserver übertragen (der evasys-Server selbst baut keine Verbindung zum Updateserver auf). Es handelt sich dabei um folgende Informationen:

* den Kundennamen
* den Lizenzschlüssel
* die aktuell betriebene evasys-Version
* die Basissprache des Systems
* die aktuell konfigurierte Sprache
* das Produktderivat
* den Inhalt der Konfigurationseinstellung „Serverhauptpfad“
* die ID des Lieferanten
* eine eindeutige ID für den Updateprüfvorgang selbst, die aus Sicherheitsgründen
* hinzugefügt wird.

All diese Informationen werden SSL-verschlüsselt übertragen und dienen ausschließlich technischen Zwecken. Es werden keinesfalls personenbezogene Daten oder Erhebungsdaten aus dem System übertragen.

**Maßnahmen gegen Standardattacken**

**Cross-Site-Scripting**

Die übertragenen Parameter (GET und POST) werden nach <script> gefiltert. Dadurch wird vermieden, dass JavaScript-Code ausführbar in das System bzw. in die Datenbank übertragen wird. JavaScript-Befehle selbst werden nicht gefiltert, da sie keine Gefahr darstellen.

**SQL-Injection**

Mit Eingabefeldern übertragene SQL-Befehle werden nicht ausgeführt, da Sonderzeichen durch entsprechende Maßnahmen maskiert werden. Somit kann ein durch ein Eingabefeld übertragener SQL-Befehl nicht ausgeführt werden.

**Penetrationstest**

Evasys wurde 2016 einem ausführlichen Penetrationstest durch ein externes Sicherheitsunternehmen unterzogen. Für den Test stand eine typische evasys-Installation auf Basis eines IIS-Webservers zur Verfügung. Die Testreihe beschränkte sich nicht nur auf die Applikation, sondern es wurde der gesamte Server mit allen Diensten geprüft, um auch beispielsweise falsche Portfreigaben zu ermitteln.

Im weiteren Verlauf der Testreihe ging es um typische sicherheitskritische Bereiche und mögliche Angriffsvektoren, wie Code Executions, SQL Injections, Cross-Site-Scripting (XSS), Information Disclosure, Sicherheit von Authentifizierung und Session sowie Cross-Site Request Forgery (CSFR), die die allgemeine Arbeit mit evasys über Browser betreffen.

Ein spezieller Testbereich war zudem die für die Anbindung an externe Systeme maßgebliche Webservice-Schnittstelle (SOAP API).

Die Testreihe wurde durchgeführt durch die Firma „SektionEins“ (https://www.sektion-eins.de/). Die Ergebnisse der Tests sind in die Entwicklung der aktuellen Version eingeflossen.

**Anlage 2** – Fragebogen