Electric Paper
EVALUATIONSSYSTEME

2018/05

Informationen zu Datenschutz und Anwendungssicherheit gemäß DSGVO - V7.1 -

Impressum

Electric Paper Evaluationssysteme GmbH

Konrad-Zuse-Allee 13
21337 Lüneburg
Deutschland

Telefon: +49 4131 7360 0
Telefax: +49 4131 7360 60
E-Mail: info@evasys.de

Geschäftsführer: Sven Meyer

USt-IdNr.: DE 179 384 158
Handelsregister: HRB-Nr. 1604, Lüneburg

Editiert von Lina Frehsdorf, Darin Gürlük, Dr. Iris Hille, Bernd Röver

Inhaltsverzeichnis

A. Datenschutz in EvaSys

1. Einleitung

In diesem Abschnitt des Dokuments sind datenschutzrechtliche Aspekte des Betriebs von EvaSys-Systemen dargelegt. Hierbei wird Bezug genommen auf die *Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46*/EG, kurz „**Datenschutzgrundverordnung**“ (DSGVO), Inkrafttretung 24.5.2016, anzuwenden ab 25.05.2018 – und auf das Bundesdatenschutzgesetz (neu) 2018 als Bestandteil des Datenschutz-Anpassungs- und -Umsetzungsgesetzes EU (DSAnpUG-EU).

1.1. Begriffsdefinitionen

1.1.1. Produktvarianten

EvaSys Education Survey Automation Suite

EvaSys-Produktvariante, in der Dozenten bzw. Trainer über passive Konten verfügen und nicht selbst auf diese zugreifen können. Der Administrator erstellt zentral sämtliche Umfragevorgänge und überwacht die Datenverarbeitung. Am Ende der Erhebungsperiode kann der Administrator die gewonnenen Daten abrufen.

Auch in der zentralen Evaluation können Dozenten- bzw. Trainerkonten aktiviert werden, mit denen Umfragen dezentral durchgeführt werden können (siehe: Nutzertypen).

EvaSys Corporate Survey Automation Suite sowie EvaSys Healthcare Survey Automation Suite

Je nach Anwendungsfall (Seminarevaluation oder allgemeine Umfragen) wird das System auf unterschiedliche Begriffswelten konfiguriert. So heißen z. B. Dozenten- oder Trainerkonten in der neutralen Sprachvariante Projektkonten, anstelle von Lehrveranstaltungen ist von Themen die Rede. Hinsichtlich des Datenschutzes verhalten sich jedoch beide Sprachvarianten identisch.

1.1.2. Nutzertypen

Administrator/in

Hauptnutzer des EvaSys-Systems, verantwortlich für die Vorbereitung, Durchführung und Auswertung von Erhebungswellen (nur zentrale Evaluation) bzw. für die Verwaltung der Nutzerkonten (zentrale und dezentrale Evaluation).

Der Administrator kann bei Bedarf, z.B. zu Vertretungszwecken, weitere Sekundäradministratoren definieren. Der Sekundäradministrator hat ebenso wie der Administrator Verwaltungsrechte für das gesamte System und kann auf alle Teilbereiche zugreifen.

Teilbereichsadministrator/in

Verantwortlich für die Vorbereitung, Durchführung und Auswertung von Erhebungswellen (nur zentrale Evaluation) bzw. für die Verwaltung der Nutzerkonten (zentrale und dezentrale Evaluation) eines oder mehrerer durch den Administrator zu bestimmender Teilbereiche.

Bei Bedarf kann der Administrator dem Teilbereichsadministrator die Einsichtsrechte in Umfrageergebnisse und/oder die Ansicht der gescannten Seiten entziehen.

Aktiviertes Dozenten- bzw. Trainer bzw. Projektkonto

Über das aktivierte Dozenten-/Trainer-/Projektkonto können Umfragen erstellt sowie später deren Ergebnisse abgerufen und ausgewertet werden.

Der Administrator hat ebenso wie ein eventuell eingerichteter und dazu vom Administrator freigeschalteter Teilbereichsadministrator Einsicht in die Umfragen und Ergebnisse des aktiven Nutzers.

Berichtersteller

Für die Erzeugung summarischer Berichte sowie für die Erstellung von Profillinienvergleichen steht der Nutzertyp Berichtersteller zur Verfügung. Dessen Zugriffsrechte können auf einen einzelnen Teilbereich und dessen Umfragen, auf eine Gruppe von Teilbereichen oder auch auf das gesamte System eingestellt werden.

Datenerfassungskraft

Die Datenerfassungskraft hat die Aufgabe, handschriftliche Kommentare von Teilnehmern an papierbasierten Befragungen zu anonymisieren, sofern die betreibende Organisation dieses Verfahren für notwendig erachtet. Es können mehrere Datenerfassungskräfte parallel über das EvaSys-Webinterface arbeiten.

Der Administrator kann den Zugriff der Datenerfassungskraft auf einen oder mehrere Teilbereiche einschränken.

Der Administrator kann der Datenerfassungskraft die Möglichkeit zur Anzeige der ganzen gescannten Fragebogenseite entziehen.

Studiendekan/in bzw. Teilbereichsleiter/in

Der Anwender dieses Nutzerprofils kann aus einer Liste von evaluierten Lehrveranstaltungen eine Auswahl treffen, die dann individuell in einem Bericht zusammengestellt wird.

Dekan/in bzw. Studienleiter/in oder Abteilungsleiter/in

Der Nutzertyp Dekan bzw. Studienleiter oder Abteilungsleiter unterscheidet sich im Vergleich zum Nutzertyp Dozent bzw. Trainer oder Projekt nur dadurch, dass eine vollständige Nutzungsstatistik für den eigenen Teilbereich dargestellt wird.

Das Nutzerkonto kann passiv oder aktiv geschaltet werden. Ein aktiver Dekan bzw. Studienleiter oder Abteilungsleiter kann ähnlich wie der aktive Dozent bzw. Trainer oder Projektverantwortliche Umfragen anlegen, Fragebögen erstellen und z.B. auf die freigeschalteten QM-Ansichten (Phase 5) zugreifen.

Mit einem passiven Konto hat der Nutzer ausschließlich Zugang zu den individuell freigeschalteten QM-Ansichten.

Verifikator/in

Der Verifikator kann für die Sichtkorrektur von gescannten Fragebögen eingesetzt werden.

Er kontrolliert die mit dem VividForms Reader verarbeiteten VividForms-Bögen und korrigiert gegebenenfalls die Erkennung. Die Verifikation kann für Umfragen aktiviert bzw. deaktiviert werden.

Dies kann notwendig sein, da unsauber ausgefüllte Bögen nicht immer maschinell korrekt gelesen werden können.

Der Verifikator hat Zugriff auf alle mit Verifikation angelegten Umfragen und Prüfungen im System. Der Administrator kann diesen Zugriff auf einen oder mehrere Teilbereiche einschränken.

Der Administrator kann dem Verifikator die Möglichkeit zur Anzeige der ganzen gescannten Fragebogenseite entziehen.

1.2. Webservice-Einstellungen

Der Konfigurationsbereich „Schnittstellen & Plug-ins“ im Hauptmenü „Einstellungen“ erlaubt im Reiter „Webservice-Einstellungen“ die Verwaltung der Verbindungen und Nutzer externer Webserver, die über die EvaSys SOAP-API Webservices mit dem EvaSys-Server kommunizieren. Die Kommunikation mit externen Webservices erfolgt verschlüsselt über SSL.

1.3. Gewährleistung der Anonymität von Umfrageteilnehmern

EvaSys ist mit zahlreichen methodischen Maßnahmen versehen, die die Anonymität von Umfrageteilnehmern garantieren.

1.3.1. Papierbasierte Umfragen

Die Fragebögen werden als Druckvorlage vervielfältigt und sind exakt identisch für alle Umfrageteilnehmer. Falls ein Fragebogen einen Umfang von mehr als einem Blatt Papier umfasst, kann eine Nummerierung der Bogensätze erfolgen, um die Zusammengehörigkeit der Einzelseiten eines Fragebogens beim Verarbeitungsvorgang identifizieren zu können.

Bitte beachten Sie: Über die Rohdaten lässt sich bei der Verwendung der laufenden Bogensatznummerierung unter Umständen der jeweilige Bogensatz genau ermitteln, da in den Rohdaten die Bogensatznummer enthalten ist. Eine Sicherstellung der Anonymität erfordert daher das anonyme bzw. zufällige Verteilen der Fragebögen.

Beim Scanvorgang werden Scans der Fragebögen erzeugt und der EvaSys-Software zwecks Auswertung der Lesezonen (Ankreuzfelder, Offene Fragen) zugeführt. Die Scans können zu Archivierungszwecken in einem in der Scanstation-Konfiguration durch den Administrator einstellbaren Netzwerkverzeichnis abgelegt werden.

Nach Extraktion der Rohdaten liegen diese als rein binäre Informationen vor. Die handschriftlichen Kommentare werden als Bildausschnitte extrahiert. Bei kleineren Befragungsgruppen ist es u.U. erforderlich, zur Wahrung der Anonymität diese Kommentare zu anonymisieren. Hierzu stellt EvaSys den Nutzertyp „Datenerfassungskraft“ zur Anonymisierung handschriftlicher Kommentare zur Verfügung. Ist die Befragungsgruppe groß genug, so kann unter Berücksichtigung des nicht unerheblichen Personalbedarfs auf eine Anonymisierung verzichtet werden. Hierzu dient eine Anonymisierungsschwelle, die den jeweiligen Rahmenbedingungen angepasst betrieben werden kann.

Die Bildausschnitte der offenen Fragen, der Datenerfassung und der Verifikation sind nicht von außen ("übers Web") zugänglich, eine Anfrage auf den Ordner ".../img" erzeugt eine "Access Forbidden (403) "- Meldung.

1.3.2. Onlineumfragen

In EvaSys kommt das so genannte TAN-Verfahren für Onlinebefragungen zum Einsatz. Hier erhalten alle Umfrageteilnehmer eine alphanumerische Zahlenkombination als Berechtigungscode zum Aufruf des Fragebogens.

Abbildung 1: TAN-Kärtchen

Diese TAN-Kärtchen können durch die Umfrageteilnehmer im Losverfahren gezogen werden. Die Umfragedaten enthalten später keinerlei Information darüber, über welche TAN ein Fragebogen ausgefüllt wurde.

Alternativ können die TANs an die Umfrageteilnehmer per Serien-E-Mail verschickt werden. Dieses Verfahren ist bei Kenntnis der E-Mail-Adressen sehr zeitsparend. Auch hier ist garantiert, dass in den Umfragedaten keinerlei Verbindung zwischen einer TAN und einem Votum hergestellt werden kann.

Teilnahmeübersicht

Die Funktion der Teilnahmeübersicht gestattet es, die Teilnahmeanonymität unter Wahrung der Befragungsanonymität aufzuheben, um z.B. bei Teilnahmeverpflichtung an Onlineerhebungen nachweisen zu können, ob eine bestimmte Person an der Umfrage tatsächlich teilgenommen hat.

Bitte beachten Sie: Es gibt hierbei keine Verbindung zwischen TAN und Votum. Es ist also nicht erkennbar, welcher Teilnehmer ***wie*** abgestimmt hat.

Diese Funktion erzeugt auf Basis einer durch den Administrator vorgegebenen Auswahl von Onlineumfragevorgängen eine CSV-Datei. Diese beinhaltet den Namen der Umfrage, die TAN, die E-Mail-Adresse an die eine jeweilige TAN verschickt wurde, sowie den Teilnahmestatus in Form einer Ja/Nein-Angabe.

Umfrage	TAN	E-Mail	Teilnahme erfolgt
Erfolgsstrategien	XQ9QW	user01@email.de	Nein
Erfolgsstrategien	TUMPM	user02@email.de	Ja
Erfolgsstrategien	1HFUR	user03@email.com	Ja
Erfolgsstrategien	CWUQN	user04@email.ch	Ja
Erfolgsstrategien	4PT95	user05@email.de	Nein
Erfolgsstrategien	NV1CW	user06@email.de	Nein
Erfolgsstrategien	R6G5E	user06@email.de	Ja
Erfolgsstrategien	MUSQS	user07@email.de	Ja
Erfolgsstrategien	VCPZT	user08@email.de	Ja
Erfolgsstrategien	YHGKV	user09@email.com	Ja
Erfolgsstrategien	R9CUW	user10@email.ch	Ja
Erfolgsstrategien	7HPTV	user11@email.de	Nein

Abbildung 2: CSV-Export des Teilnahmenachweises

Um bei sehr geringen Rücklaufzahlen zu verhindern, dass doch noch auf die Herkunft einzelner Ergebnisdatensätze geschlossen werden kann, enthält das System einen vorkonfigurierten Minimalrücklauf von fünf Fragebögen, damit überhaupt ein Teilnahmenachweis für eine betreffende Umfrage erzeugt werden kann. Der Administrator kann diese Schwelle wahlweise herauf- oder herabsetzen, wobei ausdrücklich darauf hingewiesen wird, dass ein Schwellwert von 3 oder niedriger unter Umständen die Befragungsanonymität gefährden kann.

Wahlweise kann die Funktion des Anonymitätsschutzes für die Teilnahmeübersicht den Teilbereichsadministratoren entzogen werden.

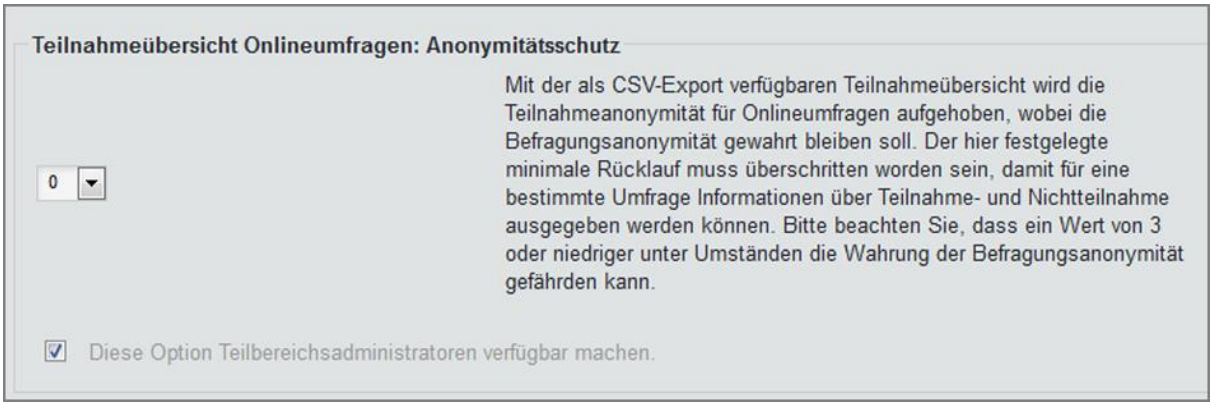

Abbildung 3: Anonymitätsschutz Teilnahmeübersicht

Rücklaufquotenbenachrichtigung

Werden Onlineumfragen zeitgesteuert durchgeführt, ist es möglich, zu einem bestimmten Zeitpunkt eine Benachrichtigung über den aktuellen Rücklauf der Umfrage zu versenden, wenn dieser einen gewissen Prozentwert unterschreitet. Diese Benachrichtigung kann an den Dozenten der Lehrveranstaltung und/oder andere Nutzer vom Typ Dekan, Dozent oder Administrator verschickt werden. Die Benachrichtigung enthält ausschließlich eine Information über die aktuelle prozentuale Höhe des Rücklaufs (z.B. 56%), d.h. der Empfänger erfährt nicht, welche Teilnehmer bereits abgestimmt haben und welche noch nicht.

Zeitstempel in den Rohdaten

Die Rohdaten enthalten den genauen Zeitpunkt der Abstimmung als Zeitstempel. Besteht Zugriff auf das Dateisystem des EvaSys Servers, kann anhand des Apache access.log (IP-Adressen) und den Rohdaten unter Umständen genau bestimmt werden, welche IP-Adresse zu einem bestimmten Datensatz gehört. Die access.log Datei sollte daher regelmäßig gelöscht werden.

1.3.3. Hybridumfragen

Bei der Hybridumfrage, einer Kombination aus Papier- und Onlineverfahren, erhalten die Teilnehmer sowohl einen Papierfragebogen als auch eine TAN zur Teilnahme an der Onlinebefragung und können wählen, welches Medium sie nutzen möchten. Es gibt zwei Wege, TANs und Fragebögen an die Teilnehmer zu verteilen:

Zum einen kann die TAN per Serien-E-Mail an die Teilnehmer verschickt werden. Es gelten die gleichen Bedingungen wie beim oben beschriebenen TAN-Versand. Im Anhang der E-Mail findet sich jedoch zudem eine PDF-Variante des Fragebogens, die alternativ zur Teilnahme an der Onlinebefragung ausgedruckt und ausgefüllt werden kann. Zum anderen kann ein Papierfragebogen an die Teilnehmer ausgeteilt werden, auf den eine TAN, ggf. auch in Form eines QR-Codes, aufgedruckt ist.

Die Papierfragebögen enthalten eine laufende Bogensatznummerierung, d.h. jeder Fragebogensatz ist nummeriert. Die Bogensatznummer eines Fragebogens ist mit der jeweils zugehörigen TAN verknüpft, so dass bei der Verarbeitung sichergestellt ist, dass ein Teilnehmer nur einen Datensatz erzeugen kann (entweder per Papier- oder per Onlineumfrage).

Bei der Verwendung des E-Mail-Versands kann in den Umfragedaten keine Verbindung zwischen TAN und Votum hergestellt werden. Bei Verteilung von Papierfragebögen ist zu beachten, dass sie, um die Anonymität zu gewährleisten, rein zufällig erfolgen muss, da ansonsten aufgrund der Bogensatznummer ein konkreter Teilnehmerdatensatz in den Umfragedaten ermittelt werden könnte.

1.3.4. Nichtanonyme Umfragen

Befragungen in EvaSys laufen standardmäßig unter Annahme und natürlich Wahrung der Anonymität der Befragungsteilnehmer ab. Falls die Identität der Befragungsteilnehmer für die Teilnehmeransprache sowie später für die Auswertung der Befragungsergebnisse benötigt werden, können aber entsprechende Teilnehmer-daten für eine Veranstaltung importiert und verwendet werden. Die Durchführung einer nichtanonymen Umfrage ist sowohl als papierbasierte als auch als Onlineumfrage möglich.

Sobald für eine Veranstaltung Teilnehmerdaten importiert wurden, geht das System davon aus, dass die Veranstaltung über nichtanonyme Umfragen ausgewertet wird. Es liegt somit in der Verantwortung des Nutzers, einen Missbrauch dieser Funktion zu verhindern.

Für einen Fragebogen für nichtanonyme Befragungen müssen im Kopf Platzhalter für die Teilnehmeridentität eingefügt werden.

EvaSys fügt bei der Versendung von Einladungen oder Erinnerungen zur Teilnahme von Onlineumfragen automatisch eine Fußnote in den E-Mail-Text ein, die jeweils Auskunft über den Umgang mit der Identität des Teilnehmers enthält.

a) E-Mail: Fußnote für Anonymität bei Onlineumfragen

HINWEIS: Diese E-Mail wurde automatisch generiert. Die in dieser E-Mail angegebene TAN ist nicht mit Ihrer Person verbunden. Ihre Stimmabgabe erfolgt anonym.

b) E-Mail: Fußnote für keine Anonymität bei Onlineumfragen

HINWEIS: Diese Umfrage ist nicht anonym. Wenn Sie unter der oben genannten TAN an der Befragung teilnehmen, können Ihre Antworten Ihnen zugeordnet werden.

Der voreingestellte Inhalt dieser Textbausteine kann nur durch den Administrator verändert werden.

1.4. Konfigurationseinstellungen

Die wichtigsten Einstellungen zur Gewährleistung einer datenschutzkonformen Verwendung von EvaSys befinden sich im Bereich „Einstellungen“ im Untermenü „Datenschutz“.

Gemäß DSGVO wird EvaSys mit einer möglichst datenschutzkonformen Grundeinstellung ausgeliefert.

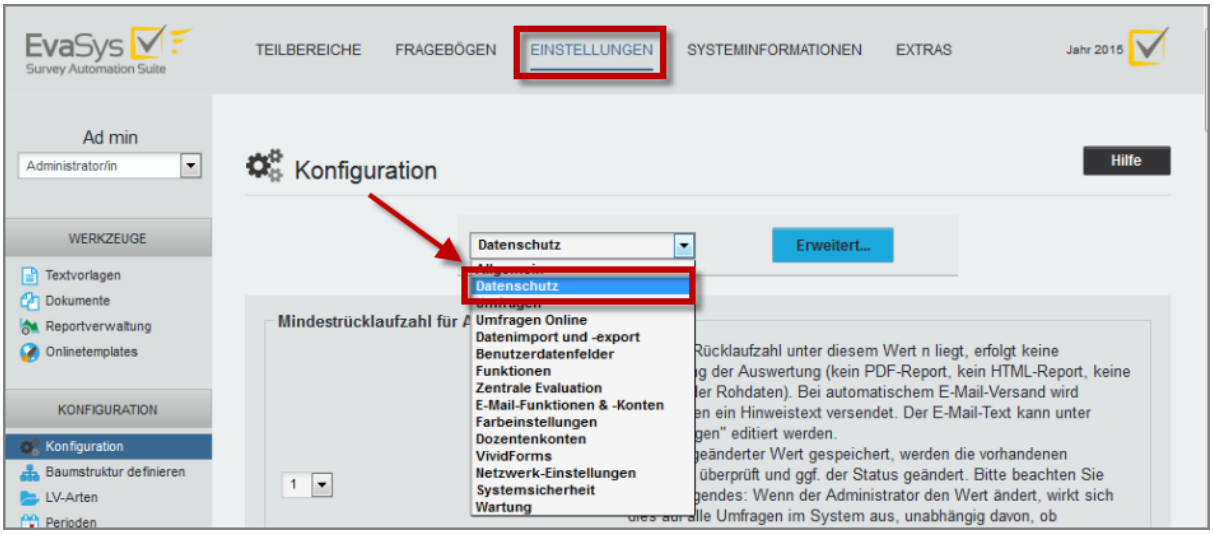

Abbildung 4: EvaSys Konfiguration

Der EvaSys Administrator kann hier systemweite Festlegungen treffen.

Teilbereichsadministratoren kann bei einigen Optionen gestattet werden, für ihre Bereiche andere Einstellungen als die systemweit festgelegten zu verwenden. Dazu wird die Checkbox bei der Option: „Diese Option Teilbereichsadministratoren verfügbar machen“ entweder aktiviert oder deaktiviert.

Auf Wunsch können die Einstellungen zum Datenschutz durch Electric Paper Evaluationssysteme GmbH gegen Veränderung gesperrt werden. Es ist dann auch dem EvaSys Administrator nicht möglich, diese Einstellungen zu ändern.

Sollen nachträglich doch Änderungen vorgenommen werden, so muss erst das Entsperren schriftlich beantragt werden. Electric Paper Evaluationssysteme wird dann die Sperre entfernen. Sind die Änderungen eingestellt, können die Konfigurationsschalter erneut gesperrt werden.

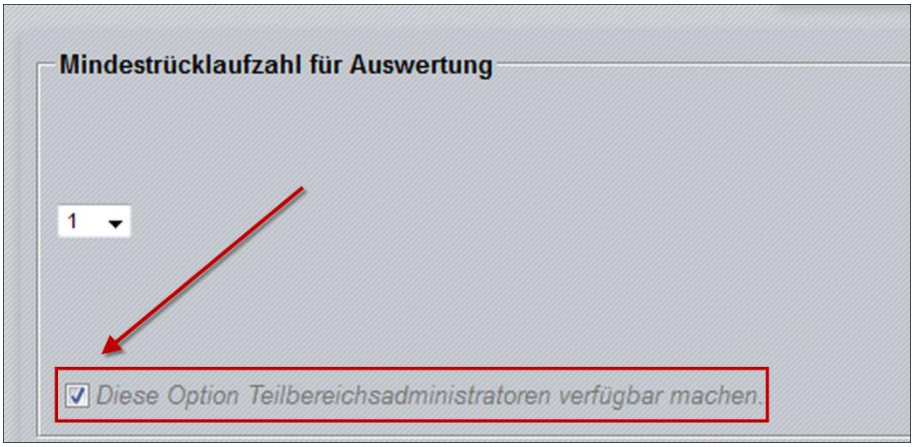

Abbildung 5: Diese Option Teilbereichsadministratoren verfügbar machen

Folgende Einstellungen stehen zur Verfügung:

Mindestrücklaufzahl für Auswertung:

Falls die Rücklaufzahl unter diesem Wert n liegt, erfolgt keine Darstellung der Auswertung (kein PDF-Report, kein HTML-Report, keine Anzeige der Rohdaten). Bei automatischem E-Mail-Versand wird stattdessen ein Hinweistext versendet. Der E-Mail-Text kann unter "Textvorlagen" editiert werden.

Wird ein geänderter Wert gespeichert, werden die vorhandenen Umfragen überprüft und ggf. der Status geändert. Bitte beachten Sie dabei Folgendes: Wenn der Administrator den Wert ändert, wirkt sich dies auf alle Umfragen im System aus, unabhängig davon, ob Teilbereichsadministratoren eigene Einstellungen vorgenommen haben. Gelten für Teilbereiche abweichende Werte, so müssen die jeweiligen Teilbereichsadministratoren anschließend ihre Einstellung erneut hinterlegen und speichern, was zur Aktualisierung der Umfragen in ihrem Bereich führt.

Mindestrücklauf bei ungewichteten Zusammenführungen beachten

Wenn aktiviert, werden Fragen, die nicht den Mindestrücklauf erreichen, nicht in die ungewichtete Zusammenführung übernommen.

Wenn deaktiviert, werden alle Fragen in die ungewichtete Zusammenführung übernommen, unabhängig davon, ob der Mindestrücklauf erreicht wurde.

Anonymisierungsschwelle

Der angegebene Wert definiert die Anzahl an Rückläufern (Fragebögen), bis zu welcher der Text von offenen Fragen zur Anonymisierung angezeigt wird. Liegt die Anzahl an Rückläufern über diesem Wert, werden die Bilder der offenen Fragen verwendet.

Wird ein geänderter Wert gespeichert, werden die vorhandenen Umfragen überprüft und ggf. der Status geändert. Bitte beachten Sie Folgendes: Wenn der Administrator

den Wert ändert, wirkt sich dies auf alle Umfragen im System aus, unabhängig davon, ob Teilbereichsadministratoren eigene Einstellungen vorgenommen haben. Gelten für Teilbereiche abweichende Werte, so müssen die jeweiligen Teilbereichsadministratoren anschließend ihre Einstellung erneut hinterlegen und speichern, was zur Aktualisierung der Umfragen in ihrem Bereich führt.

Anzeige der Teilnahmeübersicht

Wenn deaktiviert, wird der Menüpunkt "Teilnahmeübersicht" im Bereich "Zentrale Evaluation" nicht mehr angezeigt.

Teilnahmeübersicht Onlineumfragen: Anonymitätsschutz

Mit der als CSV-Export verfügbaren Teilnahmeübersicht wird die Teilnahmeanonymität für Onlineumfragen aufgehoben, wobei die Befragungsanonymität gewahrt bleiben soll. Der hier festgelegte minimale Rücklauf muss überschritten worden sein, damit für eine bestimmte Umfrage Informationen über Teilnahme- und Nichtteilnahme ausgegeben werden können. Bitte beachten Sie, dass ein Wert von 3 oder niedriger unter Umständen die Wahrung der Befragungsanonymität gefährden kann.

Löschen von Antworten offener Fragen

Aktiviert/Deaktiviert die Möglichkeit, als Administrator Antworten offener Fragen zu löschen.

Datenexport für offene Fragen zulassen

Wenn eingeschaltet, enthalten die CSV-Rohdatendateien auch die erfassten Antworten auf offene Fragen.

Anonyme Speicherung gelöschter Umfragen

Gelöschte Umfragen werden anonymisiert im Papierkorb behalten, um mit dem Berichtersteller einen akkumulierten Teilbereichsbericht generieren zu können.

Teilbereichsadministrator: Ansicht der erkannten Formulare im Original

Ist diese Option aktiviert, können sich Teilbereichsadministratoren erkannte Formulare als PDF anzeigen lassen.

Teilbereichsadministrator: Einsicht in Umfrageergebnisse

Ist diese Funktion deaktiviert, so haben Teilbereichsadministratoren keine Berechtigung, Umfrageergebnisse einzusehen oder zu exportieren.

Datenerfassungskraft/Verifikator: Anzeige der gesamten Originalseite

Wenn aktiviert, können die Datenerfassungskraft und der Verifikator die Ansicht des gesamten Bogens aufrufen.

2. Datenzugriffsrechte in EvaSys

EvaSys kann hinsichtlich der Datenzugriffsrechte frei konfiguriert werden. Die im Folgenden aufgelisteten Funktionen zeigen die vordefinierten Einstellungen, sofern Zugriffsrechte auf personenbezogene Daten betroffen sind.

Ein Häkchen ✓ symbolisiert die Verfügbarkeit der genannten Funktion. Die in Klammern angegebenen Häkchen (✓) stellen Funktionalitäten dar, die durch den Administrator ganz oder teilweise deaktiviert oder aktiviert werden können.

Beschreibung	EvaSys Survey Automation Suite
Administrator/in kann Umfragen generieren	✓
Administrator/in kann Lehrveranstaltungen/Themen verwalten	✓
Administrator/in kann zentral generierte Umfrageergebnisse einsehen	✓
Administrator/in kann aktivierte Dozenten-/Trainer-/Projektkonten und deren Umfragen und Ergebnisse einsehen	✓
Administrator/in kann Rohdaten aus Erhebungen archivieren	✓
Administrator/in kann Einsichtsrechte in Qualitätsübersichten erteilen	✓
Administrator/in kann Benachrichtigungen über auffällige Ergebnisse des Qualitätsmanagements einrichten	✓
Administrator/in kann Antworten offener Fragen löschen	✓
Administrator/in kann Antworten offener Fragen kategorisieren	✓
Teilbereichsadministrator/in kann Umfragen generieren	✓
Teilbereichsadministrator/in kann Lehrveranstaltungen/Themen verwalten	✓
Teilbereichsadministrator/in kann zentral generierte Umfrageergebnisse eines oder mehrerer bestimmter Teilbereiche einsehen	(✓)
Teilbereichsadministrator/in kann aktivierte Dozenten-/Trainer-/ Projektkonten und deren Umfragen und Ergebnisse einsehen	(✓)
Teilbereichsadministrator/in kann Rohdaten aus Erhebungen archivieren	(✓)
Teilbereichsadministrator/in kann Einsichtsrechte in Qualitätsübersichten erteilen	(✓)
Teilbereichsadministrator/in kann Benachrichtigungen über auffällige Ergebnisse des Qualitätsmanagements einrichten	(✓)
Teilbereichsadministrator/in kann Antworten offener Fragen löschen	✓
Teilbereichsadministrator/in kann Antworten offener Fragen kategorisieren	✓
Datenerfassungskraft kann ganzen gescannten Bogen einsehen	(✓)
Verifikator/in kann ganzen gescannten Bogen einsehen	(✓)

Tabelle 1: Konfiguration von Datenzugriffsrechten, Teil 1

Beschreibung	EvaSys Survey Automation Suite
Berichtersteller/in kann akkumulierte Berichte abrufen	✓
Berichtersteller/in kann komprimierte Berichte für den Prorektor/Vorstand bzw. Berichte über die Globalindikatoren erstellen	(✓)
Berichtersteller/in kann komprimierte Berichte für Dekane/Teilbereichsleiter bzw. Berichte über die Indikatoren erstellen	(✓)
Berichtersteller/in kann komprimierte Berichte für Studiendekane/Studien-leiter erstellen	(✓)
Berichtersteller/in kann Profillinien aus Berichten und Umfragen (zentrale Evaluation) vergleichen.	✓
Berichtersteller/in kann Profillinien aus Berichten und Umfragen (aktive Konten) vergleichen.	(✓)
Berichtersteller/in kann anonymisierte Teilbereichsberichte erstellen	✓
Berichtersteller/in kann anonymisierte Studiengangs-/Lehrgangs-/Gruppenberichte erstellen	(✓)
Berichtersteller/in kann Dozenten-/Trainer-/Projektprofile erstellen	(✓)
Nutzer eines aktivierten Dozenten-/Trainer-/Projektkontos sieht seinen Systemordner (zentral generierte Umfragen)	(✓)
Dekan/in bzw. Teilbereichleiter/in und Abteilungsleiter/in können automatisch Kopien von Auswertungen per E-Mail erhalten	(✓)*

Tabelle 2: Konfiguration von Datenzugriffsrechten, Teil 2

* Diese Kopien können auch ohne offene Fragen erstellt werden.

In der folgenden Tabelle sehen Sie die verschiedenen Zugriffsrechte des Administrators im Vergleich zum Teilbereichsadministrator:

Teilbereiche	Administrator	Teilbereichsadministrator
Zugriff auf Teilbereiche	Vollzugriff	Eigene(r) Teilbereich(e)
Teilbereiche hinzufügen/löschen	Vollzugriff	Kein Zugriff
Teilbereiche bearbeiten	Vollzugriff	Eigene(r) Teilbereich(e)
Nutzer erstellen, bearbeiten, löschen	Vollzugriff	Eigene(r) Teilbereich(e)
Berichte	Vollzugriff	Eigene(r) Teilbereich(e)
Archivierung	Vollzugriff	Eigene(r) Teilbereich(e)
Baumstruktur	Vollzugriff	Eigene(r) Teilbereich(e)
Umfragen generieren	Vollzugriff	Eigene(r) Teilbereich(e)
Umfragen anzeigen	Vollzugriff	Eigene(r) Teilbereich(e)
Umfragen löschen	Vollzugriff	Eigene(r) Teilbereich(e)
Meldemasken	Vollzugriff	Eigene(r) Teilbereich(e)
Serienvorgänge	Vollzugriff	Eigene(r) Teilbereich(e)
Lehrveranstaltungen/Themen anzeigen	Vollzugriff	Eigene(r) Teilbereich(e)
Geplante Vorgänge	Vollzugriff	Eigene(r) Teilbereich(e)
Datenimport	Vollzugriff	Eigene(r) Teilbereich(e)
Serienexport	Vollzugriff	Eigene(r) Teilbereich(e)
Teilnahmeübersicht	Vollzugriff	Eigene(r) Teilbereich(e)
Qualitätsmanagement-Ansichten (QM-Ansichten)	Vollzugriff	Abhängig von den Einstellungen des Administrators: Keine QM-Ansichten Nur eigene(r) Teilbereich(e) Uneingeschränkter Zugriff
QM-Reportversand	Vollzugriff	Eigene(r) Teilbereich(e)
QM-Benachrichtigungen	Vollzugriff	Eigene(r) Teilbereich(e)
Überblick über die „aktuellen Nutzer“	Vollzugriff	Vollzugriff
Fragebögen	**Administrator**	**Teilbereichsadministrator**
Fragebögen	Vollzugriff	Nur eigene Fragebögen; Fragebögen des Administrators können kopiert werden, wenn diese vom Administrator freigegeben wurden.
VividForms Editor	Vollzugriff	Vollzugriff
VividForms Designer	Vollzugriff (sofern lizenziert)	Abhängig von den Einstellungen des Administrators
Fragenbibliothek	Vollzugriff	Vollzugriff (eigene Fragen) Lesezugriff (Fragen des Administrators und öffentliche Fragen).

Tabelle 3: Datenzugriffsrechte Administrator - Teilbereichsadministrator, Teil 1

Einstellungen	Administrator	Teilbereichsadministrator
Textvorlagen	Vollzugriff	Nur Textvorlagen der eigenen Fragebögen (in den Details eines Fragebogens)
Dokumente	Vollzugriff	Nutzung vorhandener und hinzufügen eigener Dokumente
Reportverwaltung	Vollzugriff	Eigene(r) Teilbereich(e)
Onlinetemplates	Vollzugriff	Eingeschränkter Zugriff; abhängig von den Einstellungen des Administrators: Durch den Administrator festgelegt (kein Zugriff) Nur Vorlagen Uneingeschränkt
Konfiguration	Vollzugriff	Eigene(r) Teilbereich(e) Abhängig von den Einstellungen des Administrators („Diese Option Teilbereichsadministratoren verfügbar machen.“); systemweite Einstellungen können nur durch den Administrator definiert werden.
Panel-Verwaltung	Vollzugriff	Eigene(r) Teilbereich(e)
Baumstruktur definieren	Vollzugriff	Kein Zugriff
LV-/TH-Arten	Vollzugriff	Kein Zugriff
Perioden	Vollzugriff	Kein Zugriff
Nutzeranreden	Vollzugriff	Kein Zugriff
Prozessvorgaben	Vollzugriff	Eingeschränkter Zugriff
Webservice	Vollzugriff	Kein Zugriff
Sprachsets	Vollzugriff	Kein Zugriff
Eigenes Profil	Vollzugriff	Vollzugriff
Administratoren	Vollzugriff	Kein Zugriff
Organisation	Vollzugriff	Kein Zugriff
Systeminformationen	Administrator	Teilbereichsadministrator
Suchfunktion	Vollzugriff	Eigene(r) Teilbereich(e)
E-Mail schreiben	Vollzugriff	Vollzugriff
Nutzungsstatistik	Vollzugriff	Eigene(r) Teilbereich(e)
Systeminfos	Vollzugriff	Eigene(r) Teilbereich(e)
Lizenzverwaltung	Vollzugriff	Kein Zugriff
E-Mail an Support	Vollzugriff	Vollzugriff
Systembereinigung	Vollzugriff	Kein Zugriff
Systemstatus	Vollzugriff	Vollzugriff
Handbücher	Vollzugriff	Vollzugriff

Tabelle 4: Datenzugriffsrechte Administrator - Teilbereichsadministrator, Teil 2

Systeminformationen	Administrator	Teilbereichsadministrator
Beispieldateien	Vollzugriff	Vollzugriff
Zustellungen	Vollzugriff	Eigene(r) Teilbereich(e)
Logbuch	Vollzugriff	Eigene(r) Teilbereich(e) und allgemeine Logs
Löschprotokoll	Vollzugriff	Vollzugriff
Webservice Log	Vollzugriff	Vollzugriff
Mailservice Log	Vollzugriff	Vollzugriff

Tabelle 5: Datenzugriffsrechte Administrator - Teilbereichsadministrator, Teil 3

3. Datenschutzhinweise

3.1. Definition

EvaSys ist ein automatisiertes System, auf dem personenbezogene Daten gem. Artikel 4 DSGVO verarbeitet werden können.

Artikel 4 DSGVO:

"Verarbeitung" *jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das* ***Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;***

"personenbezogene Daten" *alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden* ***"betroffene Person"****) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind;*

3.2. Verantwortliche Stelle

Verantwortliche Stelle für die personenbezogenen Daten eines EvaSys-Systems ist immer die datenerhebende Stelle, also die EvaSys nutzende Organisation und nicht die Electric Paper Evaluationssysteme GmbH. Dies gilt auch für den Fall, dass das EvaSys-System von der Electric Paper Evaluationssysteme GmbH gehostet wird.

3.3. Versand von Auswertungen

EvaSys versendet E-Mails mit Auswertungen zu Umfragen an die evaluierten Personen und bietet zusätzlich Möglichkeiten, Leitungsgremien (z.B. Dekane) über die Ergebnisse einzelner Umfragen zu informieren. Als elektronisches Dokumentenformat wird dabei auf Acrobat PDF gesetzt.

Der unverschlüsselte Versand von Ergebnissen über E-Mail bedarf einer Einwilligung gemäß Artikel 7 DSGVO. Diese Einwilligung erfolgt üblicherweise über eine Betriebsvereinbarung bzw. Evaluationsordnung außerhalb von EvaSys.

Unter „Konfiguration/E-Mail Funktionen & -Konten“ lässt sich unter „Passwortschutz für per E-Mail versandte Reporte“ ein Passwort für die Verschlüsselung von versendenten PDF-Reporten hinterlegen. Ist hier ein Passwort definiert, lassen sich Reporte, die per E-Mail an Dozenten verschickt wurden, nur mit diesem Passwort einsehen. Ist das Feld leer, erfolgt kein Passwortschutz. Das Passwort gilt systemweit.

Zu beachten:

- Der Passwortschutz ist nicht PDF/A-kompatibel; PDF/A-Reporte sind daher nicht geschützt.
- Die Einstellung hat keine Auswirkungen auf den E-Mail-Versand der aktiven Nutzer.
- Passwortgeschützte Reporte lassen sich nicht mit PDF-Editoren bearbeiten.
- PDF-Report-Plug-ins, die nicht dem Standardreport entsprechen, können ggf. den Passwortschutz nicht anwenden.

Das Passwort darf maximal 32 Zeichen lang sein. Erlaubte Zeichen: a-Z, 0-9, ,;.:-_?!"$%&/()+*~#´|<>. Leerzeichen sind nicht erlaubt.

Bei Verwendung des Deckblattverfahrens kann über ein Unterschriftsfeld auf dem Deckblatt die evaluierte Person der Versendung der Ergebnisse zustimmen. Bei diesem Verfahren wird der automatisierte Versand von Reporten des Betroffenen bei fehlender Unterschrift verhindert.

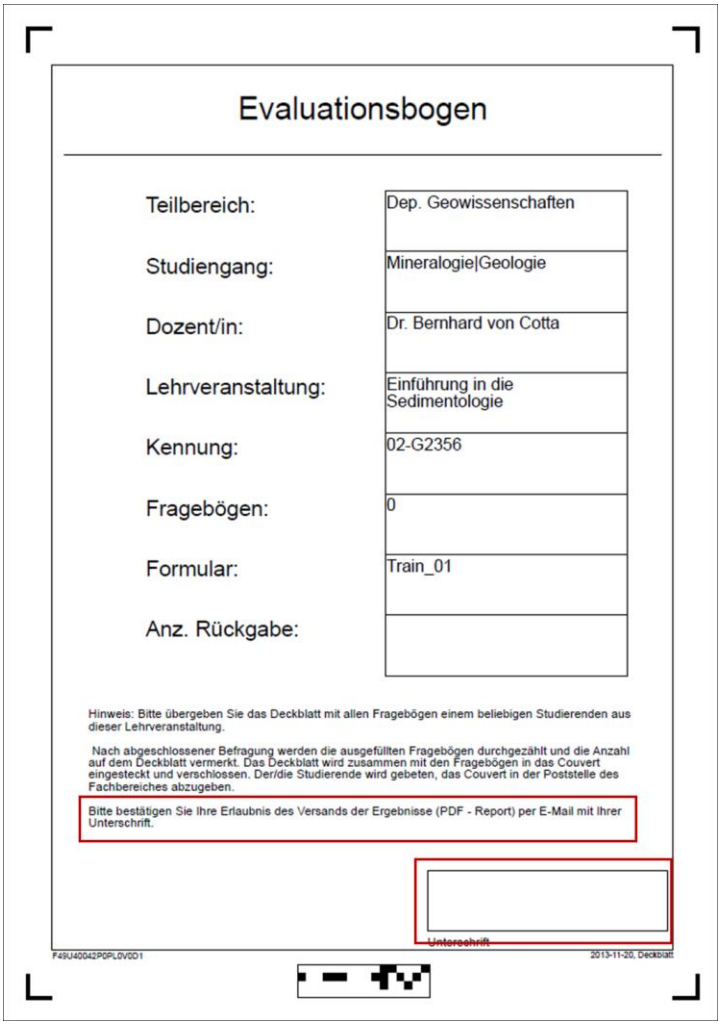

Abbildung 6: Deckblatt mit Unterschriftsfeld

Alternativ zur Versendung der Reporte per E-Mail können die Ergebnisse auch im sogenannten Pullverfahren von der evaluierten Person vom EvaSys Server abgerufen werden.

Hierbei kann eine SSL-Verschlüsselung zum Einsatz kommen.

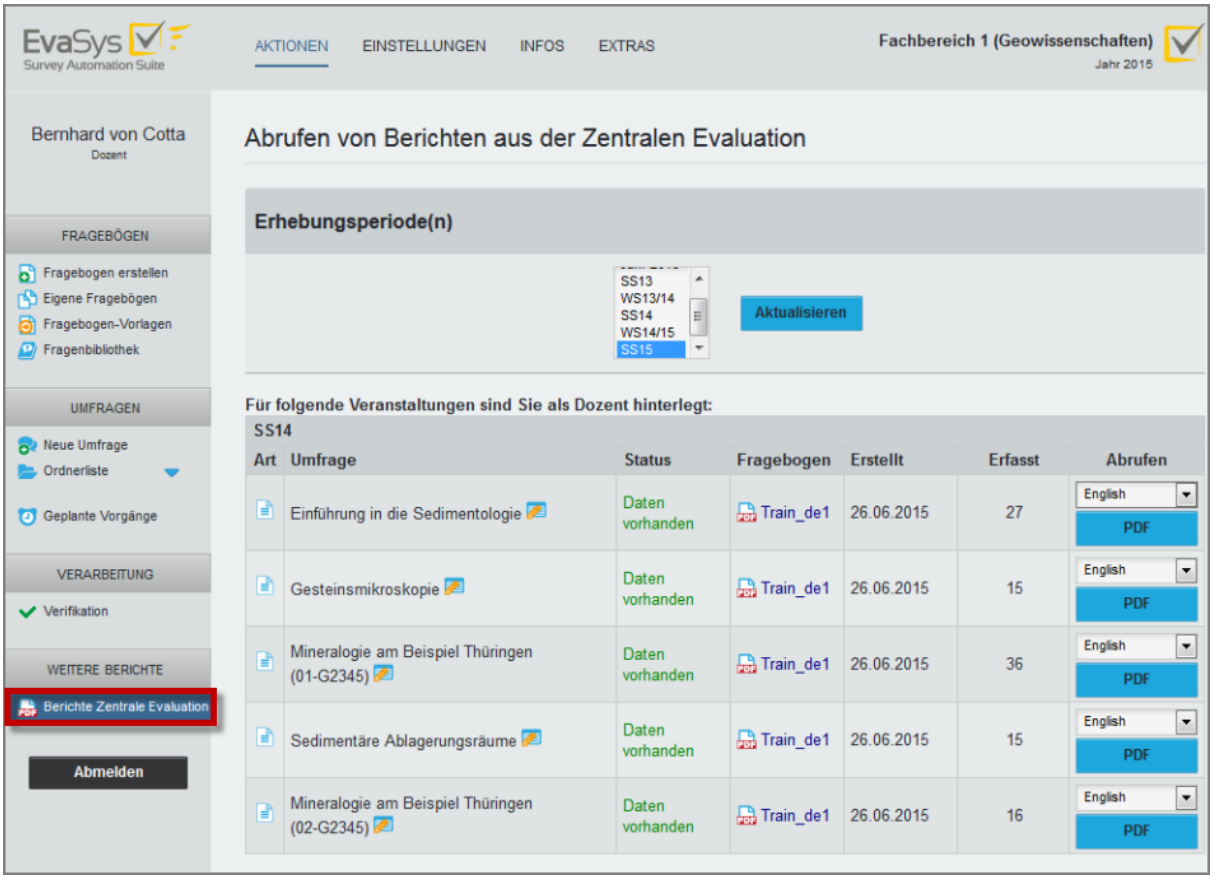

Abbildung 7: Abruf von Berichten

3.4. Verwendung von Profilbildern

Dozenten/Trainern/Projektverantwortlichen kann ein Bild zugeordnet werden. Dieses Bild kann in Onlineumfragen und auf den TAN-Kärtchen zur Teilnahme an Onlineumfragen angezeigt werden. Wird dabei ein Portrait des Nutzers gewählt, so ist darauf zu achten, dass vor Verwendung dieser Funktion in jedem Fall das Einverständnis des Nutzers einzuholen ist.

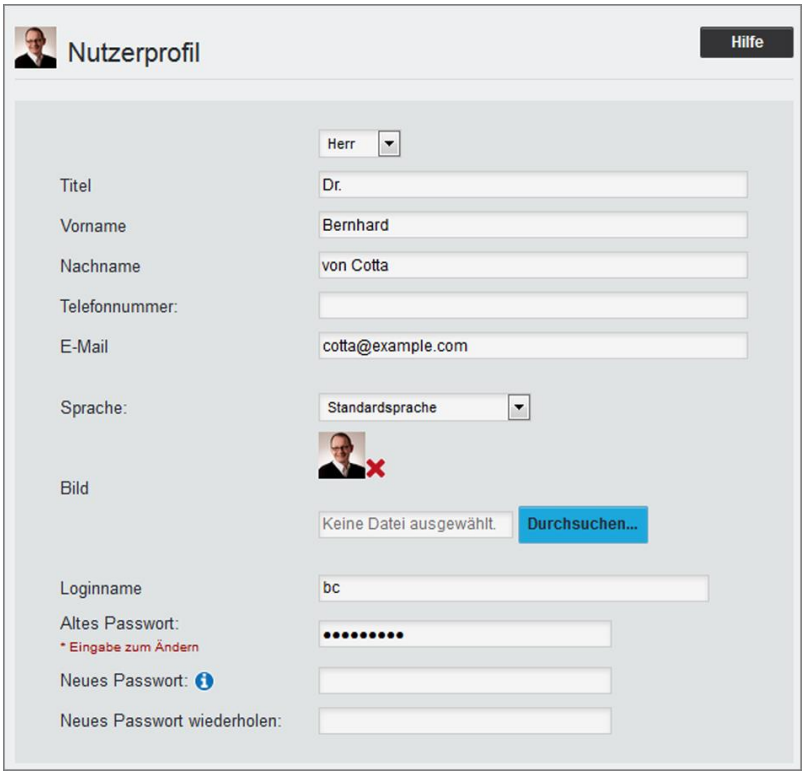

Abbildung 8: Profilbild am Dozenten

3.5. Technische und organisatorische Maßnahmen

Art. 28 DSGVO (1) Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

Im Folgenden sind die verschiedenen technischen und organisatorischen Maßnahmen in EvaSys aufgelistet.

3.5.1. Zugangskontrolle

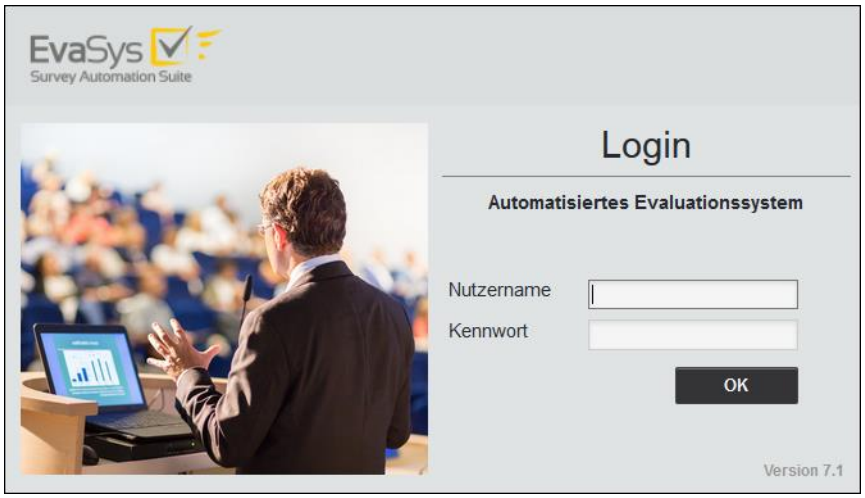

Abbildung 9: EvaSys Anmeldemaske

a) Webserver: Der Zugriff auf das EvaSys-System ist nur Personen mit einer Berechtigung in Form von Nutzernamen und Passwort möglich.
Eine Richtlinie zur Verwendung sicherer Passwörter lässt sich aktivieren. Siehe auch B.2 Maßnahmen zur Abschottung des Servers.
b) Der Zugriff auf den EvaSys-Server-PC ist nur berechtigten Personen (Nutzer auf Betriebssystemebene) über Nutzernamen und Passwort möglich.

3.5.2. Datenträgerkontrolle

Die Datenträger des Betriebssystems, auf dem EvaSys installiert wurde, sind nicht über das Netzwerk erreichbar und können lokal nur von zugriffsberechtigten Personen eingesehen werden.

Die personenbezogenen Daten in EvaSys sind in der verwendeten Datenbank (MySQL oder MSSQL) gespeichert. Die Kommunikation mit der Datenbank erfolgt in der Standardinstallation ausschließlich über den lokalen Webserver. Zusätzlich können Techniker der Electric Paper Evaluationssysteme GmbH zu Wartungszwecken indirekt auf die Datenbank zugreifen, sofern die betreibende Organisation dieses gestattet bzw. freischaltet.

3.5.3. Speicherkontrolle

Zugriff auf die erhobenen Daten haben nur Administratoren sowie Nutzer von aktivierten Dozenten-/Trainerkonten bzw. Projektkonten auf eigene Umfragen. Die Generierung von Umfragedaten erfolgt:

- bei papierbasierten Umfragen: durch Einsatz der Scanstation, die von geschulten bzw. berechtigten Personen verwendet wird. Der Zugang zu Scanstationen sollte entsprechend eingeschränkt werden. Der Konfigurationsdialog der Scanstation-Software ist aus diesem Grund passwortgeschützt.

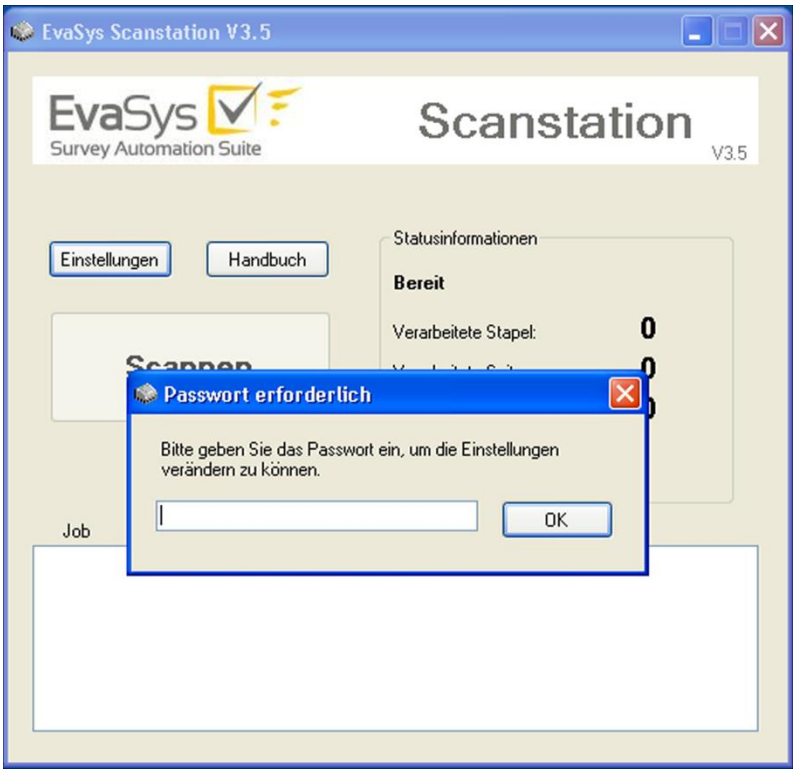

Abbildung 10: EvaSys Scanstation

- bei Onlineumfragen: Teilnehmer an Onlinebefragungen können den Fragebogen einmal ausfüllen, die Berechtigungsnummer (TAN) verfällt nach dem Einsatz.

Durch das Löschprotokoll können alle wichtigen, jemals in EvaSys vorgenommenen Löschvorgänge nachvollzogen werden. Es ist nicht möglich, Einträge aus diesem Protokoll zu löschen.

Protokolliert werden folgende Löschvorgänge:

- Teilbereiche
- Nutzer
- Lehrveranstaltungen/Themen
- Umfragen
- TANs
- Fragebögen
- Ordner (bei aktiven Dozenten/Trainern/Projekten)

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?

3.5.4. Nutzerkontrolle

Abbildung 11: Festlegen der zugelassenen IP-Adressbereiche

Der Browserzugriff ist je nach Nutzerebene auf bestimmte IP-Adressbereiche beschränkt.

So können

- Teilnehmer an Onlinebefragungen,
- Anwender von Nutzerkonten,
- der Administrator und Teilbereichsadministratoren

nur von bestimmten IP-Adressen aus zugreifen, die für jede dieser Nutzerrollen separat definiert werden können.

Der Zugriff wird erst nach Authentifikation mittels Nutzernamen und Passwort gestattet.

Die Kommunikation zwischen EvaSys-Webserver und Browserprogramm des Nutzers ist kryptographisch verschlüsselt (128-Bit SSL) und damit abhörsicher.

Durch zugriffssteuernde Maßnahmen seitens des Rechenzentrums der betreibenden Organisation wird ein wichtiger Beitrag zum Schutz des EvaSys-Systems geleistet.

Erfolgen fünf fehlerhafte Anmeldungsversuche in Folge, so wird die betreffende IP-Adresse für Logins gesperrt und anhand einer CAPTCHA-Grafik zur Eingabe einer Zahlen/Buchstabenkombination aufgefordert. Auf diese Weise werden automatisierte Verfahren zum „Erraten“ von Zugangsdaten ausgeschlossen.

Abbildung 12: Sicherheitsabfrage nach fünf erfolglosen Loginversuchen mittels CAPTCHA-Grafik

3.5.5. Zugriffskontrolle

Je nach Nutzertyp dürfen nur bestimmte Daten abgerufen werden:

Aktiviertes Dozentenkonto/Trainerkonto/Projektkonto

Nutzer kann auf die eigenen erstellten Umfragen und deren Ergebnisse zugreifen. Der Nutzer kann, sofern durch den Administrator zugelassen, auch auf die ihn betreffenden Umfrageergebnisse der zentralen Evaluation zugreifen.

Passives Dozentenkonto/Trainerkonto/Projektkonto

Ist das Dozentenkonto/Trainerkonto/Projektkonto passiv geschaltet, kann der Nutzer nur die ihn betreffenden Umfrageergebnisse der zentralen Evaluation einsehen, sofern durch den Administrator zugelassen.

Datenerfassungskraft

Der Nutzer zur Anonymisierung schriftlicher Kommentare kann zwecks Anonymisierung auf die schriftlichen Kommentare zugreifen und diese kategorisieren. Im Rahmen dieser Anonymisierung hat die Datenerfassungskraft Einsicht auf die ganze gescannte Fragebogenseite einer zu anonymisierenden Frage.

Der Administrator kann der Datenerfassungskraft die Möglichkeit zur Anzeige der ganzen gescannten Fragebogenseite entziehen.

Der Zugriff der Datenerfassungskraft lässt sich durch den Administrator auf Umfragen einer oder mehrerer Teilbereiche begrenzen.

Berichtersteller/in

Dieser Nutzertyp kann anonymisierte Teilbereichsberichte (zentrale und dezentrale Evaluation) sowie Studien-/Lehrgangs- und Dozenten-/Trainer-/Projektberichte abrufen (zentrale Evaluation).

Der Berichtersteller kann Zugriff auf einen Teilbereich, mehrere Teilbereiche oder alle Teilbereiche (systemweit) erhalten.

Teilbereichsadministrator/in

Der Teilbereichsadministrator hat vollen Zugriff auf alle zentral erhobenen Daten eines oder mehrerer bestimmter Teilbereiche.

Der Administrator kann dem Teilbereichsadministrator die Einsichtsrechte in Umfrageergebnisse entziehen. Er kann außerdem dem Teilbereichsadministrator die Möglichkeit zur Ansicht der gescannten Seiten entziehen.

Der Administrator kann dem Teilbereichsadministrator die Rolle des Berichterstellers, des Verifikators und der Datenerfassungskraft zusätzlich im selben Profil ermöglichen.

Administrator/in

Der Administrator hat vollen Zugriff auf alle erhobenen Daten. Er kann zusätzlich die Rollen des Berichterstellers, des Verifikators und der Datenerfassungskraft direkt in seinem Profil aktivieren und wahrnehmen.

Studiendekan/in bzw. Studienleiter/in (nur zentrale Evaluation)

Der Anwender dieses Nutzerprofils kann aus einer Liste von evaluierten Lehrveranstaltungen/Themen eine Auswahl treffen, die dann individuell durch den Berichtersteller in einem Bericht zusammengestellt wird.

Dekan/in bzw. Teilbereichsleiter/in oder Abteilungsleiter/in

Der Anwender hat Zugriff auf eine vollständige Nutzungsstatistik für den eigenen Teilbereich.

Das Nutzerkonto kann passiv oder aktiv geschaltet werden. Ein aktiver Dekan bzw. Studienleiter/in oder Abteilungsleiter kann seine eigenen Umfragen einsehen und z.B. auf die freigeschalteten QM-Ansichten (Phase 5) zugreifen.

Ein passives Konto hat ausschließlich Zugang zu den individuell freigeschalteten QM-Ansichten und den Umfrageergebnissen des jeweiligen Nutzers aus der zentralen Evaluation, sofern durch den Administrator zugelassen.

Verifikator/in

Der Verifikator hat Zugriff auf alle zur Sichtkorrektur freigegebenen Umfragen.

Der Administrator kann diesen Zugriff auf einen oder mehrere Teilbereiche einschränken.

Im Rahmen dieser Sichtkorrektur hat der Verifikator Einsicht auf die ganze gescannte Fragebogenseite einer zu verifizierenden Frage.

Der Administrator kann dem Verifikator die Möglichkeit zur Anzeige der ganzen gescannten Fragebogenseite entziehen.

3.5.6. Übermittlungskontrolle

Die automatische oder manuelle Zustellung von Auswertungen von Umfragen per E-Mail wird in EvaSys über die Zustellungstabelle protokolliert.

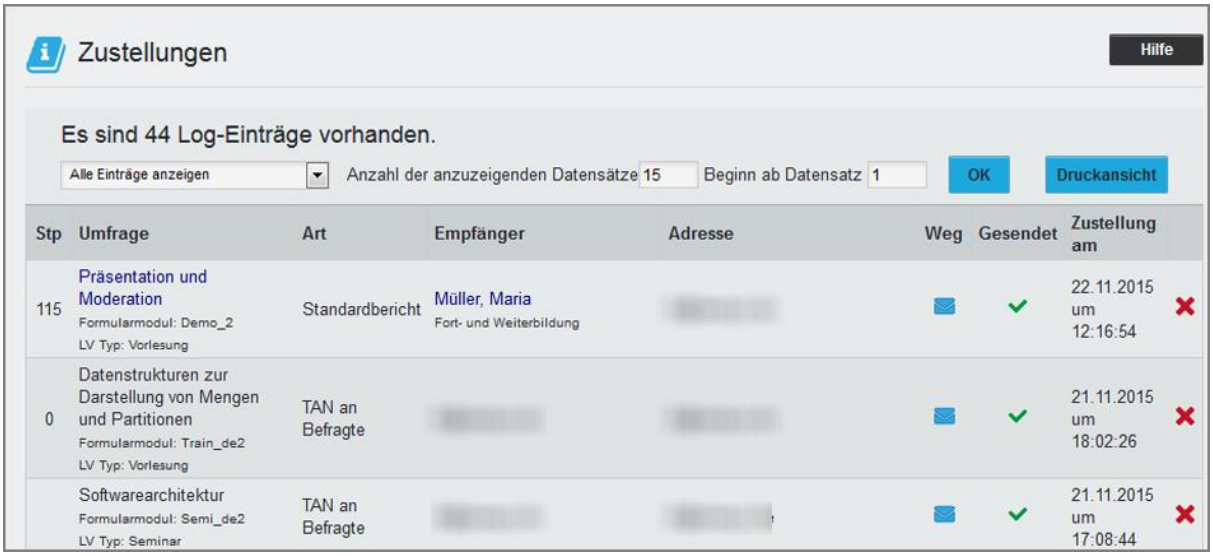

Abbildung 13: Protokoll der Zustellungen

Dabei wird der Zeitpunkt des Versandes festgehalten. Zusätzlich zu diesem Protokoll können entsprechende Protokolle des Mailservers ausgewertet werden.

Im Rahmen der Systembereinigungsfunktion lässt sich das Zustellungsprotokoll löschen.

3.5.7. Eingabekontrolle

Die Einrichtung von Nutzerkonten erfolgt nur durch den Administrator oder durch den Teilbereichsadministrator für bestimmte Teilbereiche. Der Zeitpunkt der Erstellung wird für Teilbereiche, Dozentenkonten bzw. Befragerkonten und Umfragen sowie deren Rücklaufdaten in der Datenbank festgehalten. Der Datenrückfluss von Scanstations ist durch eine Scanstation-Kennung einem Arbeitsplatz zuzuordnen, so dass auch unter Einsatz mehrerer Scanstations geprüft werden kann, von welcher Station zu welchem Zeitpunkt Daten übertragen wurden.

Jeder Zugriff auf Nutzerkonten wird durch Speicherung von Zeitstempel und IP-Adresse protokolliert. So ist nachvollziehbar, von welchem PC aus der letzte Zugriff erfolgt ist.

Das System-Protokoll des IIS- oder Apache-Webservers (access.log) verzeichnet sämtliche Zugriffe auf das System. Diese Zugriffe werden wie folgt gespeichert:

IIS:

```
2011-02-12 12:23:15 179.233.122.42 GET /evasys/umfragen.php?stuid=984&mode=show&PHP-
SESSID=533[…]49728 80 …
```

Apache:

```
179.233.122.42 - - [12/Feb/2011:12:23:15 +0100]
"GET /evasys/umfragen.php?stuid=984&mode=show&PHPSESSID=533[…]49728 HTTP/1.1" 200 4938
```

In diesem Beispiel wurde von der IP-Adresse 179.233.122.42 der Inhalt des Ordners #984 eines aktivierten Dozenten-/Trainer-/Projektkontos aufgerufen.

Bei Bedarf wäre es einem Techniker der Electric Paper Evaluationssysteme GmbH über eine Fernwartungsverbindung möglich, das verwendete Nutzerkonto zu identifizieren.

Wird ein Internet Information Server (IIS) verwendet, ist ein entsprechendes Logging der Zugriffe durch den Kunden zu gewährleisten.

3.5.8. Verfügbarkeitskontrolle

Die EvaSys-Dokumentation beschreibt die relevanten Verzeichnisse sowie Verfahren zur störungsfreien Durchführung von Systembackups (siehe Kapitel 4 - Weitere datenschutzrelevante Informationen).

3.5.9. Auftragskontrolle

Dieses liegt in der Verantwortung des Administrators bzw. der verantwortlichen Stelle.

3.5.10. Transportkontrolle

Der Kommunikationsweg zwischen dem System (Webserver) sowie dem Anwender (Browser) ist 128-Bit SSL-verschlüsselt und kann nicht abgehört oder manipuliert werden.

Erfolgt die Generierung der Umfragedaten durch den Einsatz der EvaSys Scanstation, wird die Datenübertragung erzeugter Scans ebenfalls verschlüsselt über SSL angeboten.

Die Versendung von Auswertungsdokumenten per E-Mail erfolgt aufgrund des unverhältnismäßigen Aufwandes[1] einer Kryptographielösung unverschlüsselt. Das System bietet Möglichkeiten, diesen unverschlüsselten Versand durch die betroffenen Personen schriftlich bestätigen zu lassen sowie alternativ den Postweg anzubieten.

Eine weitere Möglichkeit besteht darin, den betroffenen Personen (passive Dozenten/Trainer/Projektverantwortliche) die Ergebnisse zum Selbstabruf (Pull) SSL-verschlüsselt zur Verfügung zu stellen.

3.5.11. Organisationskontrolle

Im Vorwege der Installation von EvaSys-Systemen nimmt die Electric Paper Evaluationssysteme GmbH Kontakt zu den Rechenzentren der betreibenden Organisationen auf, um Zugriffsbeschränkungen und Aspekte des Datenschutzes zu erörtern.

[1] Um sicherzustellen, dass nur der richtige Empfänger eine Nachricht entschlüsseln kann, ist der Einsatz eines aus öffentlichen sowie privaten Schlüsseln bestehenden Verfahrens erforderlich. Jeder potentielle Empfänger muss sich selbst einen über Passwort und Zufallsfaktoren generierten privaten Schlüssel generieren sowie den gleichzeitig erzeugten öffentlichen Schlüssel an die Verschlüsselungsstelle übermitteln. Der öffentliche Schlüssel ist erforderlich, damit die Verschlüsselungsstelle die Daten so verschlüsseln kann, dass nur der Besitzer des privaten Schlüssels in der Lage ist, diese Datei wieder zu entschlüsseln. Zum Betrieb dieses Verfahrens muss die entsprechende Software (z.B. PGP – Pretty Good Privacy) auf allen PCs der Empfänger installiert sein. Die Verwaltung aller öffentlichen Schlüssel, die flächendeckende Installation der notwendigen Software sowie die Aktualisierung der Bestände erfordern einen unverhältnismäßig hohen administrativen Aufwand auf Seiten der Organisationsverwaltung sowie auch auf Seiten der Nutzer.

3.6. Auskunft (Art. 15 DSGVO Auskunftsrecht der betroffenen Person)

Der Administrator kann jederzeit Informationen über die gespeicherten Daten einsehen und Auskünfte erteilen.

Dazu steht ihm eine systemweite Suche nach Nutzern zur Verfügung:

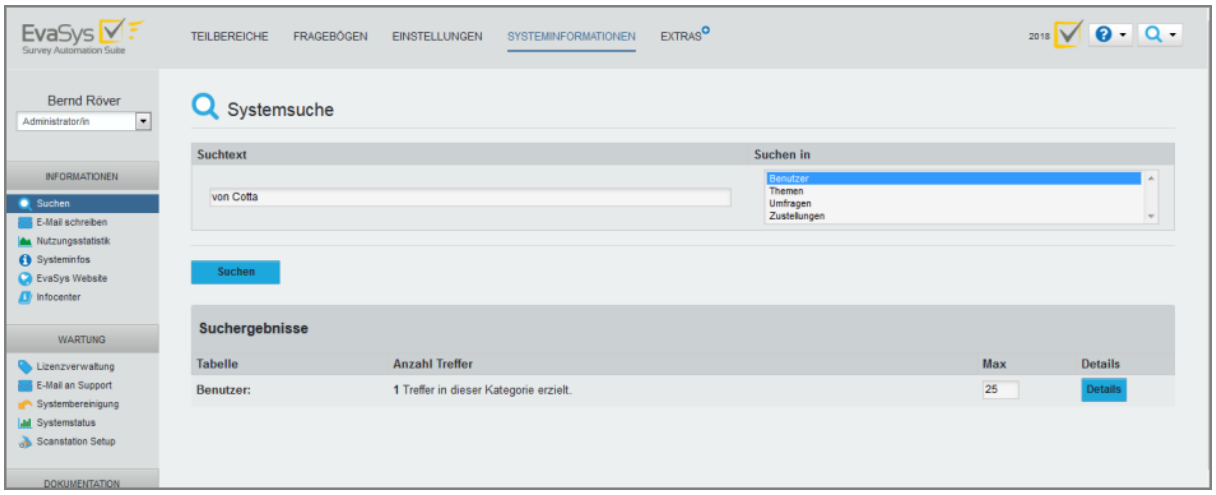

Abbildung 14: Systemweite Suche

Zur Suche von Daten von Befragungsteilnehmern hat der Administrator die Möglichkeit, im Bereich „Teilbereiche/Zentrale Evaluation/Datenimport“ die Verwaltung der Befragungsteilnehmer aufzurufen.

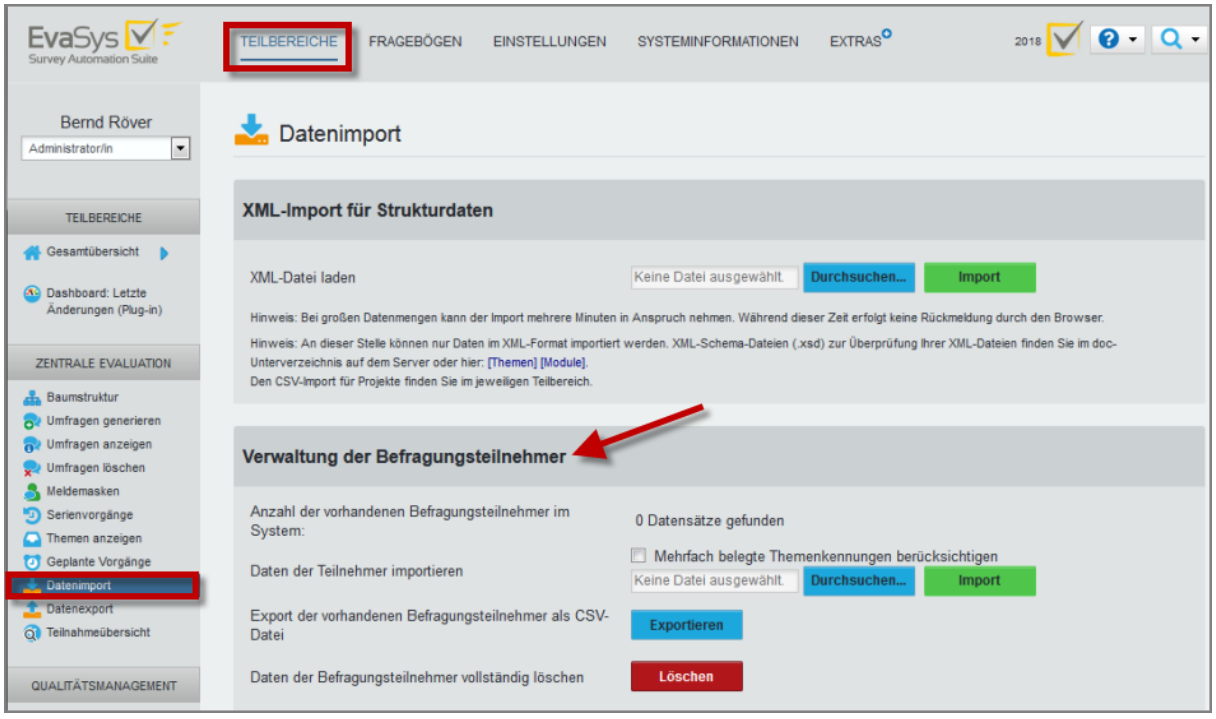

Abbildung 15: Verwaltung von Befragungsteilnehmern

3.7. Fernwartung

Die Supportmitarbeiter der Electric Paper Evaluationssysteme GmbH können zu Wartungszwecken sogenannte Fernwartungsprogramme einsetzen, mit denen eine Anreise erspart und unmittelbar mit der Beseitigung von Störungen begonnen werden kann. Diese Fernwartungsverbindung kann gemäß Spezifikation (Abschnitt 4.2) mit Teamviewer™ hergestellt werden. Die ausdrückliche Einwilligung der betreibenden Organisation ist dabei für die Herstellung der Fernwartungsverbindung stets Voraussetzung.

Die im Rahmen von Wartungsarbeiten anfallenden Datenabzüge werden nach Erledigung der Wartungsdienstleistung gelöscht.

Die Electric Paper Evaluationssysteme GmbH bietet den betreibenden Organisationen für Fernwartungszugriffe auf Anfrage eine Vereinbarung zur Auftragsdatenerfassung gemäß DSGVO an.

4. Weitere datenschutzrelevante Informationen

4.1. Backups

Um bei technischen Problemen, Hardwarefehlern oder unbeabsichtigten Löschvorgängen eine reibunglose Wiederherstellung aller wichtigen Daten sicherzustellen, müssen auf dem EvaSys-Server regelmäßig Backups durchgeführt werden. Die folgenden Komponenten müssen dabei gesichert werden:

- **Die EvaSys Datenbank**

  Die 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)

- **Grafikdateien aus offenen Fragen**

  Hierbei handelt es sich um Bildausschnitte der handschriftlich ausgefüllten offenen Fragen, die auf dem Bericht angezeigt oder der Datenerfassungskraft vorgelegt werden, als auch um Bildausschnitte, die im Verifikator angezeigt werden. Sie werden PNG-Grafikdateien in einem bestimmten Ordner auf dem EvaSys-Server gespeichert.

Für genaue Informationen zu den Ablageorten der Dateien sowie zur Erstellung von Backups vgl. Sie bitte das EvaSys Wartungshandbuch.

Im Rahmen der Papierverarbeitung kann zudem die EvaSys Scanstation-Software von jedem erfassten Fragebogenstapel eine Sicherheitskopie erstellen. Diese Sicherheitskopie wird in einem Archivordner abgelegt, der in der Scanstation definiert wird. Den genauen Pfad zum Archivverzeichnis finden Sie in den Einstellungen der Scanstation im Reiter „Scan-Ziel“. Für genauere Informationen konsultieren Sie bitte das Scanstation-Handbuch.

4.2. Fernwartung

Die Erledigung von Supportanfragen kann in den meisten Fällen schnell per Telefon oder E-Mail geklärt werden. In komplizierteren Fällen kann sich diese Methode aber als sehr langwierig und ineffektiv herausstellen. Hier empfiehlt es sich, eine Fernwartungsverbindung einzurichten.

Die Fernwartung ermöglicht es den EvaSys-Supportern virtuell bei Ihnen am EvaSys-Server zu arbeiten und die jeweilige Situation zu analysieren sowie zu lösen. Auch wird diese Verbindung ggf. zur Installation von Updates verwendet. Wichtig ist, dass mit einer solchen Fernwartung nur durch Ihre Erlaubnis eine zeitlich befristete Fernsteuerung möglich ist.

Electric Paper Evaluationssysteme GmbH verwendet hierzu die Softwarelösung „TeamViewer“. Diese Lösung funktioniert ohne Installation einer Software. Sie starten lediglich eine kleine Clientanwendung, indem Sie einen Link auf unserer Webseite anklicken:

http://support.evasys.de/OnlineSupportSystem

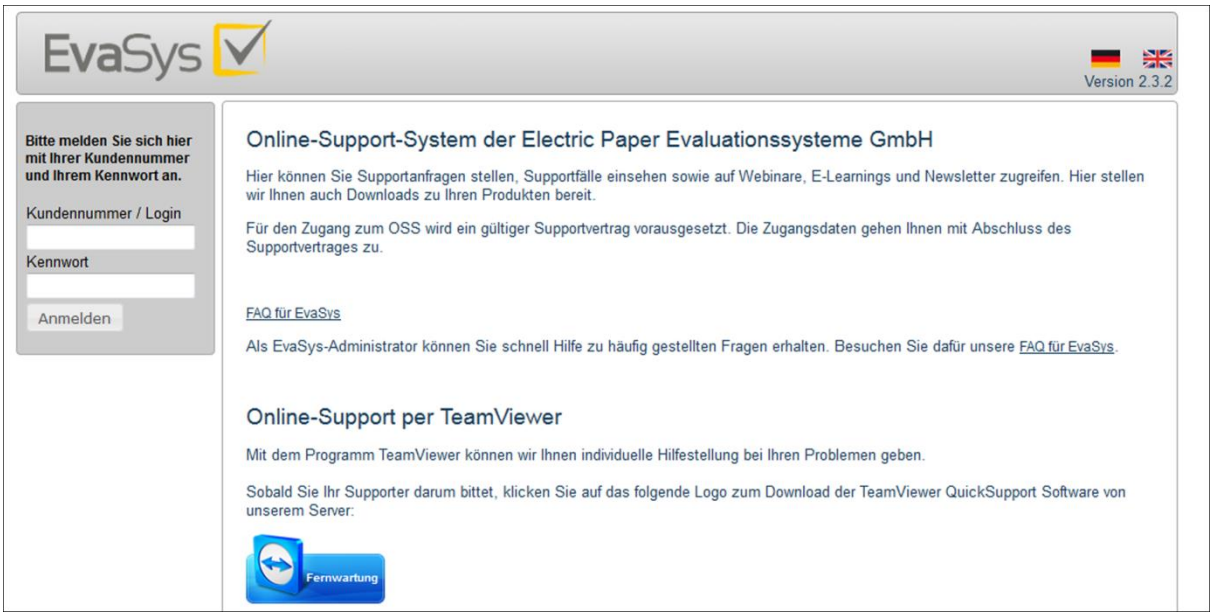

Abbildung 16: Onlinesupport

Laden Sie die Datei herunter und speichern Sie sie bzw. führen Sie sie direkt aus.

Nach dem Ausführen öffnet sich die Teilnehmer-Anwendung. Im Bereich „Ihre ID“ wird eine neunstellige ID angezeigt, im Bereich „Kennwort“ eine vierstelliges Kennwort. Teilen Sie diese ID und das Kennwort unserem Supportmitarbeiter mit, so dass er die Verbindung zu Ihrem Rechner aufbauen kann.

Abbildung 17: TeamViewer-Oberfläche

Sobald eine Verbindung zu Ihrem Rechner besteht, ist die Fernwartung aktiviert und Ihr Bildschirm wird übertragen. Sie erkennen dies an der Verbindungsübersicht, die in der rechten unteren Ecke Ihres Bildschirms angezeigt wird.

Abbildung 18: Aktivierte TeamViewer-Verbindung

Nun können Sie unseren Supportmitarbeitern bei der Arbeit zuschauen oder sich anderen Dingen zuwenden.

Sie haben jederzeit die Möglichkeit, dem Supportmitarbeiter die Kontrolle über die Maus zu entziehen, indem Sie auf die Schaltfläche mit dem blauen Pfeil neben dem Mitarbeiternamen klicken.

Alternativ klicken Sie auf den Pfeil neben dem Mitarbeiternamen und deaktivieren Sie die Option „Steuerung zulassen“. Sie können die Sitzung zudem durch Klicken auf das Kreuz bzw. Auswahl der Option „Verbindung schließen“ beenden.

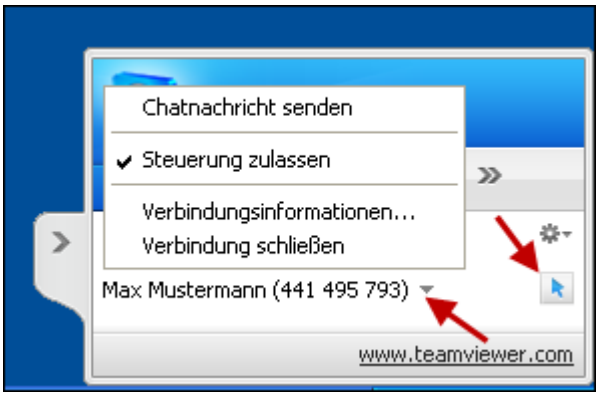

Abbildung 19: Fernsteuerung beenden

Sobald die Wartung beendet ist, wird der Supportmitarbeiter die Verbindung schließen.

Näheres zu Sicherheitsfragen finden Sie auf der TeamViewer-Website.

4.3. 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.

Sollten Sie mit der Übertragung dieser Informationen nicht einverstanden sein, kann die Funktion in der Systemkonfiguration unter „Einstellungen/Konfiguration/Wartung/ Automatische Update-Überprüfung“ deaktiviert werden. Sie werden auch unabhängig von dieser Funktion auf anderem Wege über verfügbare Updates informiert werden.

Nutzen Sie als Administrator eine sichere https-Verbindung zum Server und ist in EvaSys der Serverhauptpfad ebenfalls mit https versehen (z.B. https://example.com/ evasys), gleichzeitig aber kein sicheres Zertifikat auf dem Server installiert/das installierte SSL-Zertifikat ungültig, so wird die Update-Prüfung nicht funktionieren. Je nach Browser erscheint nach dem Login eine vom Browser stammende Warnmeldung.

Da der Einsatz nicht sicherer Zertifikate auch an anderen Stellen Probleme verursacht und Browser generell empfehlen, eine Verbindung zu einem Server mit unsicherem Zertifikat nicht aufzubauen, wird dringend empfohlen ein sicheres Zertifikat zu beschaffen. Weiterführende Informationen zu Zertifikaten Ihrer Organisation erhalten Sie in der Regel bei Ihrer IT-Abteilung.

4.4. Installation mit Mandanten

Eine Sonderform der EvaSys-Systeminstallation ist die so genannte Mandanteninstallation. Auf einem (vorhandenen) Basissystem werden weitere Unterinstallationen vorgenommen, so dass mehrere Organisationen über eine gemeinsame technische Infrastruktur evaluieren können.

Die Mandanteninstallation beinhaltet serverseitig eine eigene Datenbank sowie eine eigene Webserveradresse für jedes Mandantensystem. Somit verfügt jeder Mandant über eine eigene Datenbasis, eigene Einstellungen und eine eigene Nutzerverwaltung.

Da technisch betrachtet alle Mandanten ein und dieselbe Formularauswertungssoftware verwenden, müssen alle Vorgänge mandantenübergreifend verwaltet werden. Dieses geschieht über eine Masterdatenbank. Der Administrator der Masterdatenbank (Serverbetreuer) kann auf alle Vorgänge zugreifen, die aufgrund einer uneindeutigen Kennzeichnung keinem Mandanten zugeordnet werden konnten. Damit kommt dem Administrator des Hauptsystems eine betriebssichernde Rolle über Mandantengrenzen hinweg zu.

Folgende Sicherheitsmerkmale sind gegeben:

- Die Mandanten sind voreinander geschützt. Es kann nach dem erfolgreichen Login auch nicht durch Kenntnis der Webadresse der anderen Mandanten ein Login „erschlichen“ werden.
- Die Datenbankzugangsdaten sind verschlüsselt, so dass auch der Systembetreuer nicht auf die Erhebungsdaten zugreifen kann.
- Jeder Mandant kann eigene IP-Adressbereiche definieren, so dass sich organisationsfremde Personen nicht am Mandantensystem anmelden können, obwohl es sich physikalisch in einem anderen Netzwerk befindet.
- Die Bilder aus offenen Fragen sind im Dateisystem des Servers vorhanden und können theoretisch durch den Systembetreuer eingesehen werden. Deshalb erfüllt der Systembetreuer auch eine Vertrauensfunktion.

- Die Archivierung der digitalen Bilder gescannter Fragebögen kann an der jeweiligen Scanstation direkt erfolgen. Falls also die Scanstation dezentral aufgestellt wurde, erfolgt die Archivierung ebenfalls dezentral.

4.5. Hostingsysteme

Wird das EvaSys System auf einem von Electric Paper Evaluationssysteme GmbH zur Verfügung gestellten und gewartetem Server verwendet (sogenanntes Hosting), so ist eine Vereinbarung zur Auftragsdatenverarbeitung (ADV) gemäß DSGVO Bestandteil des Vertrags.

Electric Paper Evaluationssysteme seinerseits fordert für Server, die zum Hosting bei entsprechenden Providern angemietet werden, eine solche Vereinbarung enstprechend EU-DSGVO.

Der Datenschutzbeauftragte der Electric Paper Evaluationssysteme GmbH überprüft regelmäßig die vom Provider getroffenen technischen und organisatorischen Maßnahmen.

Die Server, die von Electric Paper Evaluationssysteme GmbH für das Hosting für deutsche Organisationen (Kunden) verwendet werden, stehen ausschließlich in Deutschland. Die Daten werden nicht in Drittländer übermittelt.

B. Anwendungssicherheit von EvaSys

1. Einleitung

In diesem Abschnitt des Dokuments wird die Sicherheit von EvaSys in Bezug auf unerwünschte Eingaben und die Konfiguration des Webservers Apache beschrieben.

2. Maßnahmen zur Abschottung des Servers

- Der EvaSys-Server ist ausschließlich aus dem Verzeichnis /evasys ansprechbar.
- EvaSys erzeugt absolute Links auf die im System angegebene Adresse.
- Der Webordner (htdocs) des Apache Servers kann nicht eingesehen werden und ist vor Zugriff von außen geschützt.
- Zugriffe auf den beiliegenden MySQL Server sind nur über „localhost“ möglich, SQL Abfragen von anderen Systemen innerhalb des Netzwerkes werden nicht zugelassen. Ausnahme: Die Datenbank liegt auf einem anderen Server, dann ist genau die zusätzliche IP erlaubt. Bei der Installation der EvaSys-Datenbank auf einem MSSQL-Server liegt die Zugriffskontrolle und Verantwortung für diese beim Kunden.
- Der Apache Webserver lädt nur Module, die zum Betrieb von EvaSys notwendig sind. Es werden keine unnötigen Module geladen. Dies reduziert die Anfälligkeit des Servers gegenüber Standardattacken und Skripts. Wird EvaSys auf einem Internet Information Server (IIS) vom Kunden installiert, hat der Kunde für die sichere Konfiguration seines Servers die Verantwortung.
- Die Kommunikation zum Server kann vollständig über eine verschlüsselte Verbindung (SSL) abgewickelt werden, sowohl für die eigentlichen Nutzer als auch für die Onlineteilnehmer.
- Sämtliche http- und https-Zugriffe werden vom Apache Server geloggt und können durch gängige Tools ausgewertet werden, z.B. für Zugriffsstatistiken.
- Sichere Passwörter: Bei der Anlage von Passwörtern wird die Sicherheit des gewählten Passwortes angezeigt. Zudem lässt sich in der Konfiguration das Verwenden von sicheren Passwörtern erzwingen. Dann wird ein Passwort mit einer Mindestlänge von 8 Zeichen gefordert, das mindestens einen Großbuchstaben, einen Kleinbuchstaben und eine Zahl enthält. Dabei dürfen nicht mehr als zwei aufeinander folgende Zeichen identisch sein.

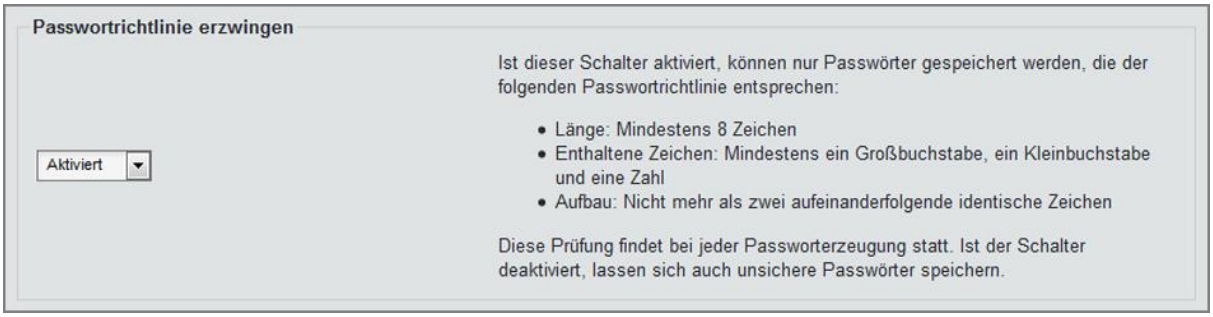

Abbildung 20: Passwortrichtlinie erzwingen

3. Aktualisierung der Serverkomponenten

Die Electric Paper Evaluationssysteme GmbH ist für die Aktualisierung der installierten Applikationen, wie Apache, MySQL und PHP verantwortlich. Electric Paper erhält Informationen der Hersteller der einzelnen Applikationen, um Sicherheitsupdates schnellstmöglich bereitstellen zu können. Vom Kunden bereitgestellte MSSQL und Internet Information Server (IIS) müssen durch den Kunden selbst gewartet werden, da sie von der Electric Paper Evaluationssysteme GmbH weder installiert noch gewartet werden können.

4. Maßnahmen gegen Standardattacken

4.1. 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.

4.2. 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.

4.3. 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.

5. Filterung unerwünschter Eingaben

5.1. Filterung im Allgemeinen

Durch Eingabefelder übertragene Sonderzeichen werden maskiert, um Standardattacken entgegen zu wirken. Darüber hinaus werden übertragene Tags wie z.B. <script> in der Regel gefiltert oder durch Maskierung unterdrückt.

5.2. Filterung in Onlineumfragen

Alle HTML-Tags in den zu übertragenen Werten der Formulare werden herausgefiltert. Die über die URL übermittelten Parameter (GET) können nicht dazu verwendet werden, die Datenbank zu kompromittieren bzw. Schadcode auszuführen. Versuche, den Login der Onlineumfrage mit SQL-Injection zu überwinden, bleiben ohne Konsequenzen. Es werden keine näheren Angaben zur Datenbank angezeigt.