Technisches und rechtliches Rezertifizierungs-Gutachten - Kurzgutachten -

Einhaltung datenschutzrechtlicher Anforderungen durch das IT-Produkt "stepnova Version 4.48"

für:

ergovia GmbH, Kiel

erstellt von:

Andreas Bethke
Dipl. Inf. (FH)
Beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein anerkannter Sachverständiger für IT-Produkte (technisch)

Papenbergallee 34
25548 Kellinghusen
tel 04822 – 36 63 000
fax 04822 – 36 63 333
mob 0179 – 321 97 88
email bethke@datenschutz-guetesiegel.sh

Stephan Hansen-Oest
Rechtsanwalt
Beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein anerkannter Sachverständiger für IT-Produkte (rechtlich)

Neustadt 56
24939 Flensburg
tel 0461 – 90 91 356
fax 0461 – 90 91 357
mob 0171 – 20 44 98 1
email sh@hansen-oest.com

Stand:
10.01.2018

A. Einleitung

Die ergovia GmbH (nachfolgend: ergovia) strebt die Rezertifizierung ihres Produktes „stepnova“ für das Gütesiegel für IT-Produkte des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) an.

Die Vorlage eines rechtlichen und technischen Gutachtens ist Voraussetzung für die Rezertifizierung des Produktes. Dieses Dokument dient als Gutachten zur Vorlage beim ULD im Zusammenhang mit der Rezertifizierung des Produktes.

Dem Gutachten wird der Anforderungskatalog in der Version 2.0 zugrunde gelegt.

Das Gutachten stellt die Zusammenfassung der von den Sachverständigen vorgenommenen Prüfungen dar und berücksichtigt insbesondere die Neuerungen/Änderungen des Produktes sowie eine etwaige geänderte Rechtslage. Auf die Unterlagen, die im Zusammenhang mit der Erstzertifizierung vom 15.10.2014 zugrunde gelegt wurden, wird Bezug genommen.

B. Zeitpunkt der Prüfung

Die Prüfung des Produktes fand vom 30.05.2016 bis zum 10.01.2018 statt.

C. Detaillierte Bezeichnung des IT-Produktes

Das Produkt „stepnova“ ist ein webbasiertes System zur Organisation im Bildungssektor. Es dient der Unterstützung von Maßnahmen für die berufliche Bildung und wird bei der elektronischen Maßnahmeabwicklung (eM@w) der Bundesagentur für Arbeit, sowie für Jobcentermaßnahmen (z.B. für die berufliche Weiterbildung) und von Bildungseinrichtungen eingesetzt.
Das Produkt wird in fünf Varianten vertrieben (Professional Edition, Basic Edition, Starter Edition, Stepfolio Edition und Refugee Edition.).
Nicht zum Gegenstand der Zertifizierung gehört das sog. „stepnova-Addon“. Ebenfalls nicht zum Gegenstand der Zertifizierung gehört die „stepfolio-App“.

D. Änderungen und Neuerungen des Produktes

Mit der Version 4.48 von stepnova wurden folgende datenschutzrelevante Änderungen gegenüber der Version 4.22 identifiziert:

1. Allgemeine Änderungen

Im Arbeitsbereich „Teilnehmerdaten“ wurde bei den Personenstammdaten das Feld "Geburtsname" neu mit aufgenommen. Es handelt sich nicht um ein Pflichtfeld.
Es wurde die Möglichkeit geschaffen, die Auswahlmöglichkeit der Standorte für bestehende und neue Benutzerdaten noch weiter einzuschränken. Dazu kann man nun in der Administration eine Standortfreigabe für bestehende Benutzer tätigen. Diese Einschränkung der Standortauswahl bezieht sich nur auf den Bereich der Personaldaten, d.h. auf die zur Verfügung stehenden Standorte bei der Einrichtung eines neuen oder Änderung eines bestehenden Benutzerkontos. Statt sämtliche Standorte zur Auswahl anzubieten, kann ein Administrator der Software nun die Auswahl begrenzen
Besonders geschützte Einträge im Arbeitsbereich „Beratung“ (Freigabe zum Beispiel nur für ein Konto) sind nun durch alle Benutzer erkennbar. Es wird dargestellt, dass es ein zugriffsbeschränkter Eintrag ist, wer die Eintragung vorgenommen hat und wann dies geschah. Weitere Inhalte sind nur für autorisierte Benutzer einsehbar.
Kennwortsicherheitsoption: "Kennwörter müssen Groß- und Kleinbuchstaben enthalten", die Option wurde standardmäßig für alle Kunden aktiviert
Die Funktionalität der Löschung/Anonymisierung wurde zur Erfüllung der Nachweispflicht gegenüber der BA durch die Kunden um ein Protokoll erweitert, das die folgenden Daten enthält:

- Lfd.Nr.
- Nachname
- Vorname
- TeilnehmerID
- Produkt
- Produktzeitraum

Dieses Protokoll wird vom Hersteller nicht gespeichert, sondern dem Anwender einmalig nach Abschluss der Anonymisierung/Löschung zur Verfügung gestellt. Dies soll dem Anwender als Nachweis dienen und ist Anforderung vieler Kunden des Herstellers.

Die Ausgabe eines Eintrags aus dem AB_Portfolio enthält nun auch das Alter eines Kindes zum Zeitpunkt der Erstellung des Eintrags.
Die Auswahl des Geschlechts einer Person wurde erweitert um die Option "X - Unbestimmt"

2. Änderungen in den Arbeitsbereichen

a) **Edition Refugees**
Es wurde ein neuer Arbeitsbereich „Refugees“ erstellt, der in der „Edition Refugees“ eingebettet ist.
Dieser Arbeitsbereich enthält mehrere Unterpunkte. Er dient ehrenamtlichen Helfern und Verbänden als ein System, um die Stammdaten eines Geflüchteten aufzunehmen und diesem einen Kurs zuzuordnen. Für die Kurse gibt es eine Verwaltung der Lehrkräfte. Ferner ist eine einfache Benutzerverwaltung enthalten.
Hiermit werden die Benutzer für die Refugee-Edition verwaltet. Die Anwender dieser Edition haben keinen Zugriff auf den Bereich Personaldaten der anderen stepnova-Editionen. Die Daten werden in denselben Strukturen abgelegt und entsprechend gleich verwaltet. Auch die Grundeinstellungen für die Kennwortsicherheit sind analog zu den anderen Editionen (Kennwortlänge von zehn Zeichen, Kombination aus Zahlen und Buchstaben muss vorliegen, mindestens ein Sonderzeichen, ein Groß- und ein Kleinbuchstabe, halbjährliche Änderung). Jedoch gibt es für diese Edition keinen Administrator, d.h. diese Einstellungen können nicht mehr geändert werden.
Für einen Benutzer werden in dieser Edition nur die folgenden Daten erfasst.

Benutzerdaten

- Status aktiv / inaktiv
- Vorname
- Nachname (Pflichtfeld)
- E-Mail-Adresse (Pflichtfeld) -> erforderlich für die Kennwort-E-Mails
- Benutzername für den Login (Pflichtfeld)

Der Benutzer kann sein eigenes Kennwort ändern. Dazu wurde die Funktionalität der Kennwort-Ändern-Maske aus den anderen Editionen vollständig integriert. Der Benutzer muss also sein aktuelles Kennwort eingeben, das neue wiederholen und er bekommt eine Visualisierung der Kennwortstärke.

Zu den **Teilnehmerdaten** gehören

- vollständiger Name (einziges Pflichtfeld)
- Geschlecht
- Geburtstag, wobei Tag und Monat optional sind
- Geburtsort
- Staatsangehörigkeiten
- Straße, Hausnummer, Postleitzahl, Ort, Postfach und ein Zusatz zur Adresse
- Telefonnummer
- E-Mail-Adresse
- Einreisedatum
- Aufenthaltsstatus gemäß Asylgesetz

Zusätzlich kann optional ein Ansprechpartner des Verbandes hinterlegt werden. Dessen Daten bestehen aus dem Geschlecht, Vor- und Nachname und einer Telefonnummer.
Für spezielle Bedürfnisse, wie Kinderbetreuung während des Kursbesuchs oder der Besuch eines Kurses ausschließlich für Frauen, gibt es 2 weitere Erfassungsfelder.

Zur Vermittlung in Kurse gibt es Merkmale. Diese sind

- Sprachniveau
- Erfassung, ob eine Einstufungstest durchgeführt wurde und wenn ja, wann
- Erfassung, ob ein Sprachtest durchgeführt wurde und wenn ja, wann
- Erfassung, ob ein Zertifikat für ein Sprachniveau vorliegt und wenn ja, für welchen Level
- Grad der Alphabetisierung
- Lerntempo
- Förderbedarf

Als letztes wird noch die Verfügbarkeit eines Teilnehmers erfasst. Die Verfügbarkeit ist statisch nach Wochentagen in Zeitabschnitte aufgeteilt. Der Benutzer kann an einem ausgewählten Wochentag einen Zeitabschnitt anlegen und hat dazu die Startzeit und Endzeit des Abschnitts variabel. Freitextfelder sind hier nicht existent.

Zudem werden **Daten der Lehrkräfte** (Mitarbeiter der Träger und Verbände) verarbeitet:

- Geschlecht
- vollständiger Name (Pflichtfeld)
- Anschrift (zwecks geographischer Einordnung in Beziehung zum Kursort)
- Telefon
- E-Mail-Adresse
- Einsatzregion
- Beruf

Eine Lehrkraft erhält zur Zuordnung zu einem Kurs ebenfalls Merkmale, die denen der Teilnehmer entsprechen. Die Semantik der Merkmale ist nur aus Sicht der Lehrkraft, d.h. sie ist z.B. in der Lage, einen Kurs mit Sprachzielniveau B1 zu geben.
Ferner werden die Verfügbarkeiten der Lehrkraft in Stundenblöcken an allen Werktagen inklusive Samstag erfasst.
Für die Teilnehmer gibt es eine entsprechende Einwilligungserklärung, die der Hersteller dem Kunden mit an die Hand gibt. Die Einwilligungserklärung erfüllt die Voraussetzungen von § 4a BDSG und auch Art. 6 Abs. 1 lit. a) und Art. 7 der Datenschutz-Grundverordnung (DSGVO).
Außerdem gibt es für diese Edition einen separaten Lizenzvertrag mit entsprechender Auftragsdatenvereinbarung.

b) Edition stepfolio

Die stepfolio-Edition wurde vertraglich in 4 Editionen light, basic, basic+ und premium aufgeteilt, wobei basic+ nicht zum Zertifizierungsgegenstand gehört.
Den Editionen wurden die Arbeitsbereiche „Anwesenheit“ und „Beratung“ hinzugefügt und unterscheiden sich sonst nur durch die Anzahl der verfügbareren lizensierten oder

individuellen Beobachtungsbögen und durch unterschiedliche Servicequalität (nur E-Mail vs. persönliche Betreuung).
Der Arbeitsbereich „Portfolio“ wurde geändert, dass die Fotos nun zum Standardumfang der stepfolio-Edition gehören. Im Datenschutz-Merkblatt wird allgemein von Personenfotos gesprochen – es gibt weiterhin ein Modul, welches Teilnehmerportraits beinhaltet und das weiterhin standardmäßig zu keiner Edition zugehörig ist.

Die Verwendung der Fotofunktion in der Software ist optional. Die Funktion dient nicht der Veröffentlichung von Fotos. Gegen die Verwendung dieses Features gibt es auch keine datenschutzrechtlichen Bedenken. Diese Funktion dient vor allem der Verlaufsdokumentation und der Dokumentation des Entwicklungsstandes eines Kindes. Die Kindertagesstätten haben einen Betreuungs-, Erziehungs- und Bildungsauftrag. Nach § 4 Abs. 2 des Schleswig-Holsteinischen Gesetzes zur Förderung von Kindern in Tageseinrichtungen und Tagespflegestellen (Kindertagesstättengesetz - KiTaG) sind in den Kindertagesstätten Fähigkeiten entsprechend dem jeweiligen Alter und Entwicklungsstand zu unterstützen und weiterzuentwickeln. Um diese Aufgabe wahrzunehmen ist nach § 4 Abs. 3 Nr. 1 KiTaG auch eine Beobachtung und Dokumentation des Zustandes von Körper und Gesundheit eines Kindes zu berücksichtigen. Hierbei kann eine Verlaufsdokumentation auf Basis von Fotos sehr hilfreich und damit zur Aufgabenerfüllung erforderlich sein. Dies gilt insbesondere dann, wenn die Betreuung durch mehrere Personen einer KiTa erfolgt.
Die jeweilige KiTa hat Sorge dafür zu tragen, dass das für das Anfertigen des Fotos erforderliche Einverständnis der zuständigen Personen vorliegt. Festzustellen ist jedoch, dass die Funktion der Software datenschutzkonform eingesetzt werden kann.

Ferner gibt es im AB_Portfolio nun die Möglichkeit, Einträge mit anderen Einträgen aus dem AB_Individuell zu verknüpfen. Dies ist sinnvoll, um Beobachtungen zu Lernerfolgen bei Kindern durch ein Portfolio belegen zu können.

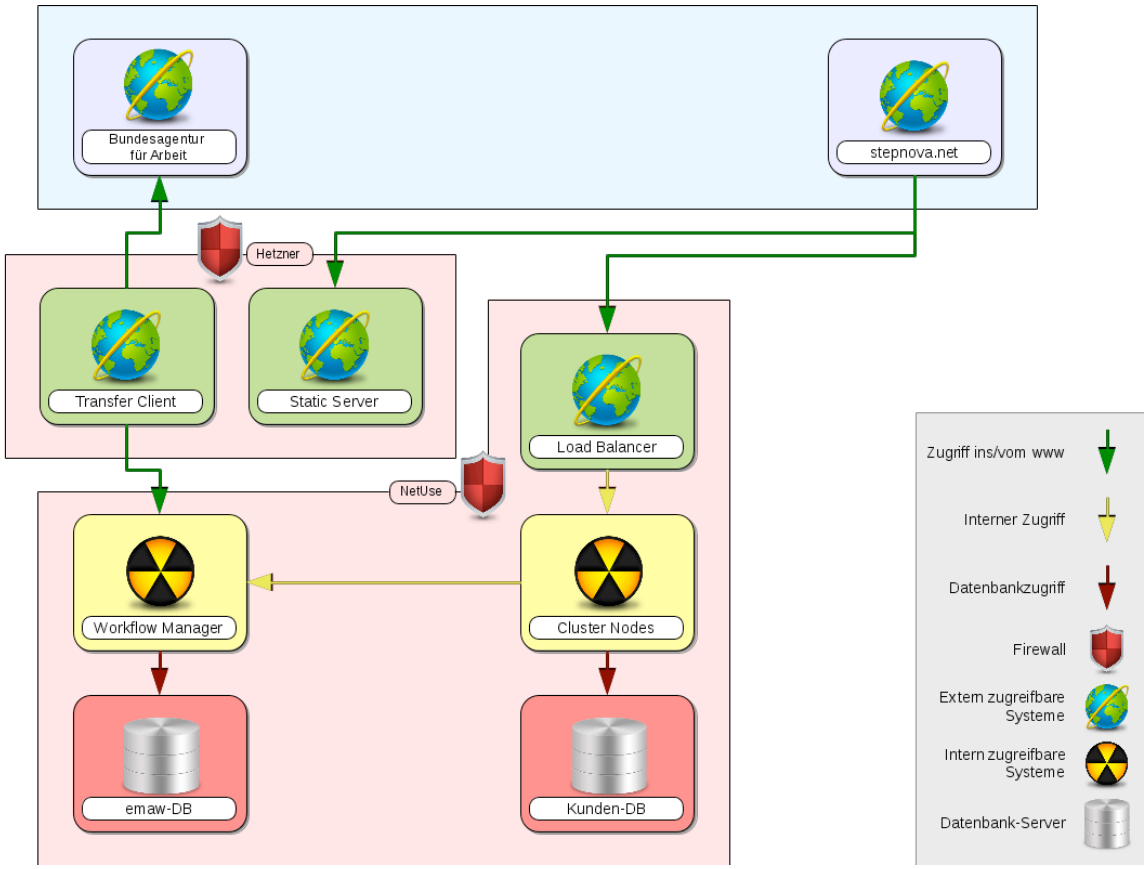
3. Änderungen an den Infrastruktur-Komponenten

Durch das Patch- und Releasemanagement des Herstellers, werden die Systeme permanent aktualisiert. Zum aktuellen Zeitpunkt (Versionsstand 4.48) wurden folgende Komponenten seit der Erstzertifizierung aktualisiert

- Webserver (Patch des OS-Kernels und Wechsel der Webserverkomponente von Apache auf nginx)
- Tomcat-Anwendungsserver (wurde auf die aktuelle Version aktualisiert)
- Datenbankserver (wurde auf die aktuelle Version aktualisiert)
- Jumpserver (hier wurde die OpenSSH-Komponente aktualisiert und auch die OpenSSL-Komponente)

4. Änderungen am Datenfluss

Seit der Erstzertifizierung wurde der Static-Server aus dem NetUse-Rechenzentrum ins Hetzner-Rechenzentrum verschoben. Somit ergibt sich eine Änderung im Datenfluss.



5. Änderungen im Bereich Auftragsdatenverarbeitung

Zum Zeitpunkt der Erstzertifizierung setzte der Hersteller für die Systemwartung des Online-Servers die Firma MARE System aus Kiel als Unterauftragsdatenverarbeiter ein. Die geschäftliche Verbindung ist gelöst und ergovia hat die Aufgaben selbst übernommen. Insoweit wurde der Auftragsdatenverarbeitungsvertrag entsprechend abgeändert. Weitere Änderungen am Auftragsdatenverarbeitungsvertrag hat es nicht gegeben. Insoweit kann auf die Ausführungen im Erstgutachten verwiesen werden.

6. Änderungen in der Außendarstellung (Produktseiten)

Der Aufruf für das Portal hat sich nicht geändert. Dies ist nach wie vor unter https://www.stepnova.net/login.do bzw. https://stepfolio.net/login.do zu erreichen. Jedoch gibt es neue Produktseiten, auf denen weitergehende Produktinformationen abgerufen werden können:

- https://stepnova.de/ gilt für die Editionen Professional, Basic und Starter
- https://stepfolio.de/ gilt für die Edition stepfolio
- https://izel-digital.de/ gilt für die Edition stepfolio-IzEL
- https://fluechtlingskurse.de/ gilt für die Edition Refugees

7. Änderungen im Datenschutzmerkblatt

In der aktuellen Version des Datenschutzmerkblattes, das für die Kunden im Kundenportal hinterlegt ist, wird auf die Erfassung von Nutzungsdaten, wie z.B. die aufgerufene URL, hingewiesen.

8. Änderungen bei der Protokollierung (gem. § 6 LDSG SH)

Um Änderungen an Datensätzen nachvollziehen zu können, müssen diese durch das IT-Produkt protokolliert werden. In der aktuellen Version des Produktes wird zu jedem Datensatz das Erstelldatum, die Benutzerkennung des Erstellers, sowie das Änderungsdatum und ebenfalls die dazugehörige Benutzerkennung gespeichert. Sofern eine Änderung durchgeführt wird, werden die Daten in einer Revisionstabelle festgehalten. Einen Zugriff auf diese Protokolldaten erhalten die Benutzer nur mit Hilfe des Herstellers. Hierfür wurde ein entsprechender Prozess aufgesetzt.

9. Vertragliche Änderungen

Der Hersteller hat Änderungen an den Lizenzverträgen vorgenommen. Die neuen Verträge sind vom rechtlichen Sachverständigen geprüft worden. Diese enthalten keinerlei Aspekte, die für eine datenschutzrechtliche Bewertung von Belang wären.

E. Datenschutzrechtliche Bewertung

In technischer Hinsicht könnten die Änderungen durchaus positiv bewertet werden. Der Wegfall des Unterauftragnehmers MARE vermindert das Risiko durch eine bessere Zugangs- und Zugriffskontrolle.
Das Release- und Patchmanagement hält die Komponenten der Infrastruktur aktuell. Die Verbesserung im Bereich der Protokollierung (gem. § 6 LDSG SH) wird positiv bewertet.

In rechtlicher Hinsicht hat es keine Änderungen der einschlägigen rechtlichen Vorschriften gegeben. Insoweit war eine Neubewertung nicht erforderlich.

Seit der letzten Rezertifizierung wurde der Anforderungskatalog des ULD Gütesiegels angepasst. Darum soll an dieser Stelle die neue tabellarische Darstellung erfolgen.

Anforderung nach Katalog oder sonstigen Rechtsnormen	**Bewertung**	**Kommentare**
Komplex 1:		
1.1 IT-Sicherheits-Schutzziele: Verfügbarkeit, Integrität, Vertraulichkeit	vorbildlich	
1.2 Datenschutz-Schutzziel: Nicht-Verkettbarkeit (inkl. Datensparsamkeit, Zweckbindung und Zwecktrennung)	adäquat	
1.3 Datenschutz-Schutzziel: Transparenz (inkl. Produktbeschreibung)	adäquat	
1.4 Datenschutz-Schutzziel: Intervenierbarkeit	adäquat	
1.5 Anpassung des IT-Produkts	vorbildlich	
1.6 Privacy by Default	vorbildlich	
1.7 Sonstige Anforderungen	entfällt	
Komplex 2:		
2.1.1 Gesetzliche Ermächtigung zur Verarbeitung der Daten	adäquat	
2.1.2 Einwilligung des Betroffenen	adäquat	
2.1.3.1 Vorschriften über die Datenerhebung	adäquat	
2.1.3.2 Vorschriften über die Übermittlung	adäquat	
2.1.3.3 Löschung nach Wegfall des Erfordernisses	adäquat	
2.2.1 Zweckbindung und Zweckänderung	adäquat	

Anforderung nach Katalog oder sonstigen Rechtsnormen	Bewertung	Kommentare
2.2.2 Erleichterung der Umsetzung des Trennungsgebotes	adäquat	
2.2.3 Gewährleistung der Datensicherheit (§§ 5, 6 LDSG, Anlage zu § 9 BDSG)	adäquat	-
2.3 Datenverarbeitung im Auftrag	adäquat	-
2.4.1 gemeinsame Verfahren/Abrufverfahren	adäquat	-
2.4.2 Trennung der Verantwortlichkeiten	adäquat	-
2.4.3 Veröffentlichungen im Internet	adäquat	
2.4.4 Weitere besondere technische Verfahren	adäquat	
2.5.1 Erleichterung bzw. Unterstützung von Pseudonymität und des Pseudonymisierens	adäquat	
Komplex 3:		
3.1.1. Physikalische Sicherung	adäquat	
3.1.2 Authentisierung	adäquat	
3.1.3 Autorisierung	adäquat	
3.1.4 Protokollierung	adäquat	
3.1.5 Verschlüsselung und Signatur	adäquat	
3.1.6 Pseudonymisieren	entfällt	
3.1.7 Anonymisieren	entfällt	
3.2.1.1 Verfügbarkeit	vorbildlich	
3.2.1.2 Integrität	vorbildlich	
3.2.1.3 Vertraulichkeit	adäquat	
3.2.1.4 Nicht-Verkettbarkeit	adäquat	
3.2.1.5 Transparenz	adäquat	
3.2.1.6 Intervenierbarkeit	adäquat	
3.2.1.7 Protokollierung von Datenverarbeitungsvorgängen	adäquat	
3.2.1.8 Test und Freigabe	adäquat	
3.2.2 Erleichterung der Vorabkontrolle	adäquat	
3.2.3 Erleichterung bei der Erstellung des Verfahrensverzeichnisses	adäquat	
3.2.4 Benachrichtigungspflicht bei unrechtmäßiger Kenntniserlangung von Daten	entfällt	
3.2.5 Unterstützung der Tätigkeit des behördlichen Datenschutzbeauftragten		
3.3.1 Verschlüsselung	adäquat	
3.3.2 Anonymisierung oder Pseudonymisierung	entfällt	
3.3.3.1 Mobile Datenverarbeitungssysteme	entfällt	
3.3.3.1 Video-Überwachung und –Aufzeichnung	entfällt	
3.3.3.1 Automatisierte Einzelentscheidungen	entfällt	
3.3.3.1 Veröffentlichungen im Internet	entfällt	
3.4 Pflichten nach Datenschutzverordnung (DSVO), insbesondere für Verfahren	adäquat	
3.5 Anforderungen an den Betrieb bei Auftragsdatenverarbeitung	adäquat	
3.6 Sonstige Anforderungen	entfällt	
Komplex 4:		
4.1 Aufklärung und Benachrichtigung	adäquat	
4.2 Benachrichtigung des Betroffenen bei unrechtmäßiger Kenntniserlangung von Daten	adäquat	
4.3 Auskunft	adäquat	
4.4.1 Berichtigung	adäquat	

Anforderung nach Katalog oder sonstigen Rechtsnormen	Bewertung	Kommentare
4.4.2 Vollständige Löschung	adäquat	
4.4.3 Sperrung	adäquat	
4.4.4 Einwand bzw. Widerspruch gegen die Verarbeitung	adäquat	
4.3.5 Gegendarstellung	adäquat	
4.5 Sonstige Anforderungen	entfällt	

F. Zusammenfassung

Insgesamt kann festgestellt werden, dass auch mit dem neuen Produkt die Rechtsvorschriften zu Datenschutz und Datensicherheit eingehalten werden.

Hiermit bestätige ich, dass das oben genannte IT-Produkt den Rechtsvorschriften über den Datenschutz und die Datensicherheit entspricht.

Kellinghusen, den 10.01.2018

Andreas Bethke

Flensburg, den 10.01.2018

Stephan Hansen-Oest