Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des Innern EDI

Eidgenössische Büro für die Gleichstellung von Frau und Mann (EBG)

Sicherheitsdeklaration

Standard-Analyse-Tool (Logib)
Nachweis zur Sicherheit

1 Kontext

Nach Art. 13c Abs. 2 Gleichstellungsgesetz (GIG) stellt der Bund den Arbeitgebenden für die Durchführung von Lohngleichheitsanalysen ein kostenloses Standard-Analyse-Tool zur Verfügung. Arbeitgebende, die Lohngleichheitsanalysen nach Art. 13a GIG mit diesem Standard-Analyse-Tool durchführen, können mit der vorliegenden Konformitätserklärung den Nachweis einer im Sinne von Art. 13c Abs. 1 GIG wissenschaftlichen und rechtskonformen Methode erbringen (s. Art. 7 Abs. 3 Verordnung über die Überprüfung der Lohngleichheitsanalyse). Das Standard-Analyse-Tool (Logib) wurde vom Eidgenössischen Büro für die Gleichstellung von Frau und Mann (EBG) zu Beginn der 2000-Jahre mit Unterstützung privater spezialisierter Institutionen entwickelt. Seit 2020 wird Logib als Webapplikation durch das EBG vom Bundesamt für Informatik und Telekommunikation (BIT) betrieben.

1.1 Nachweis der Sicherheit

Eine Schutzbedarfsanalyse sowie der IKT-Grundschutz wurden gemäss den Sicherheitsvorgaben (IKT-Grundschutz) erstellt und in Kraft gesetzt. Im Anhang sind die Vorkehrungen zur Gewährung der Sicherheit transparent und vollständig aufgezeigt.

Hiermit bestätigt das Eidgenössische Büro für die Gleichstellung von Frau und Mann EBG, dass das Standard-Analyse-Tool (Logib) allen Sicherheitsvorgaben des Bundes gemäss Schutzbedarfsanalyse und IKT-Grundschutz entspricht. Mit der Webapplikation werden keine besonders schützenswerten Daten verarbeitet. Die Webapplikation wird regelmässig gewartet und auf Sicherheitslücken geprüft.

Bern, Oktober 2020

Aeberhard Patric PURVAM
Digital unterschrieben von Aeberhard Patric PURVAM
Datum: 2020.10.20 08:14:01 +02'00'

Sylvie Durrer	**Markus Grossenbacher**	**Patric Aeberhard**
Direktorin EBG	Leiter Sicherheit BIT	Lohngleichheitsexperte EBG

Anhang zur Sicherheitsdeklaration

Status	in Arbeit, in Prüfung, genehmigt
Version	2020.2

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

2 Einführung zur Sicherheitsdeklaration

Dieses Dokument zeigt eine Übersicht der Sicherheitsmassnahmen, welche für das Standard-Analyse-Tool (Logib) angewendet werden. Ab Kapitel 3.1 werden diese detailliert in einem Frage- und Antwortformat beschrieben.

2.1 Was ist Logib?

Logib [1] ist das Standard-Analyse-Tool des Bundes für Lohngleichheitsanalysen.

Das Eidgenössische Büro für die Gleichstellung von Frau und Mann (EBG) in Zusammenarbeit mit dem Bundesamt für Informatik und Telekommunikation (BIT) entwickelten Logib weiter, damit Arbeitgebende einerseits im Selbsttest die Einhaltung der Lohngleichheit zwischen Frauen und Männern überprüfen und andererseits Kontrollen im Beschaffungswesen (Art. 8 Abs. 1 Bst. c BöB) durchgeführt werden können.

2.2 Das revidierte Gleichstellungsgesetz: Art. 13a ff. GIG

Ab dem 1. Juli 2020 ist das revidierte Gleichstellungsgesetz (GIG) in Kraft getreten, d.h. Unternehmen ab 100 Mitarbeitenden müssen alle 4 Jahre eine Lohngleichheitsanalyse durchführen und diese von einer unabhängigen Stelle überprüfen lassen. Weiter sind Arbeitnehmende sowie Aktionärinnen und Aktionäre über das Ergebnis der Lohngleichheitsanalyse zu informieren. Zusätzlich tritt eine Verordnung in Kraft, die die Ausbildung der Revisionsunternehmen, die Überprüfung der Lohngleichheitsanalysen sowie den Zeitplan regelt [2]. Somit ist der Bund verpflichtet, allen Arbeitgebenden ein kostenloses Standard-Analyse-Tool gemäss Art. 13c Abs. 2 GIG ab dem 1.Juli zur Verfügung zu stellen.

2.3 Nachweis der Sicherheit

Eine Schutzbedarfsanalyse [3] sowie der IKT-Grundschutz [4] wurden gemäss den Sicherheitsvorgaben (IKT-Grundschutz) erstellt und in Kraft gesetzt.

2.4 Kurzer Beschrieb der Sicherheitsdeklaration

Nachfolgend werden die wichtigsten Punkte dieser Sicherheitsdeklaration kurz aufgelistet:

- Die Daten stehen/der dem Anwendenden nur in der aktuellen Browsersession zur Verfügung und werden daher nirgends permanent gespeichert.
- Die Daten können nur lokal im Browser Cache des Users bearbeitet werden. Dritte haben keinen Zugriff darauf.
- Sobald der Browser geschlossen wird, werden alle Daten gelöscht.
- Die Daten werden über https resp. verschlüsselt übertragen.
- Der Server von Logib wird vom Bundesamt für Informatik und Telekommunikation betrieben.
- Die Anwendung Logib basiert auf wissenschaftlichen und rechtskonformen Methoden [5].

3 Architektur

In diesem Kapitel wird die Architektur und deren technische Umsetzung skizziert.

3.1 Übersicht von Logib

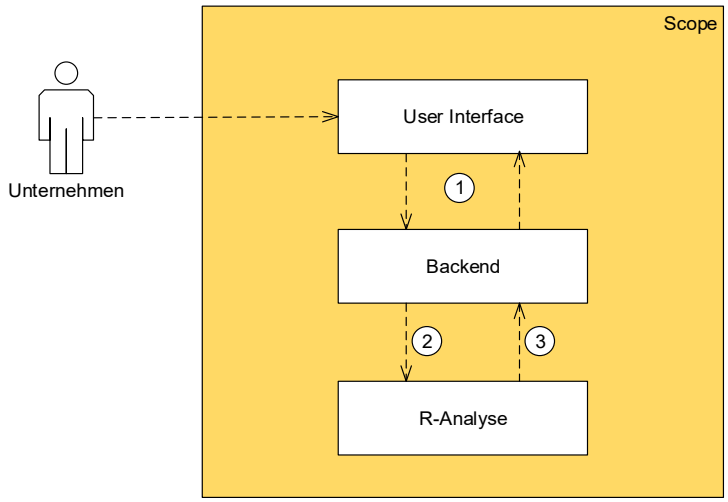

Abbildung 1: Übersicht Logib

3.2 Worauf basiert Logib technisch?

3.2.1 User Interface

Diese Komponente dient der Interaktion mit dem Benutzer.

Im vorliegenden System (Etappe 2), muss sich der Benutzer nicht anmelden.

- Plausibilitätsprüfung der eingereichten Daten (ausser Laufnummer-Validierung)
- Syntaktische Prüfung der eingereichten Daten
  →https://confluence.bit.admin.ch/pages/viewpage.action?pageId=268097910
- Daten von der Analyse Komponente (R) grafisch aufbereiten mit der JavaScript SW-Bibliothek Highcharts

Produkt/Technologie

Oblique/ Angular sind das Frontend-Framework.

Die beiden Bausteine User Interface und Backend werden zusammen in einem Microservice realisiert.

3.2.2 Backend

Im Backend Modul werden primär folgende Funktionen ausgeführt:

- Auslesen des Datenfiles und Umwandlung in ein JSON File
- Transformation Alter, Geschlecht, Dienstjahr
- Validierung der Laufnummer (aus Performancegründen nicht auf UI)
- Die Daten werden im JSON Format an R gesendet und wiederum als JSON von R empfangen

Produkt/Technologie

.NET Core 3.x
→Freie und quelloffene Software-Plattform der .NET-Plattform, die zur Entwicklung und Ausführung von Anwendungsprogrammen dient und unter der Koordination von Microsoft entwickelt wird.

Die beiden Bausteine User Interface und Backend werden zusammen in einem Microservice realisiert und sind in demselben Container enthalten.

3.2.3 R-Analyse

Die Komponente R-Analyse als Backend kümmert sich rein um die Berechnungen (Basis für: Standardisierung der Löhne, Regressionsanalyse, Cockpit-Zahlen). Es werden keine Grafiken, Tabellen, etc. aufbereitet.

Die Daten werden vom Backend als JSON-File übergeben.

Die Ergebnisse nach den Berechnungen werden ebenfalls als JSON wieder an das Backend zurück geliefert.

Details zu den Attributen sind in der Detailbeschreibung der Schnittstellen zu finden, Kap. 4.1.2 Datenfluss.

Produkt/Technologie:

- Plumber (REST API) für die Kommunikation der Bausteine Backend und R-Analyse.
- Der Baustein R Analyse wird in einem eigenen Container implementiert.

3.3 Wo stehen die Server?

Die Server stehen in den geschützten Rechenzentrumsräumen des Bundesamtes für Informatik und Telekommunikation in der Schweiz.

3.4 Wie ist der Zugriff auf Logib möglich?

3.4.1 Interner Zugriff

Systemadministratoren sowie Entwickler und Tester der Anwendung haben zwangsläufig über eine personalisierte User Rolle Zugang zur Applikation.

3.4.2 Externer Zugriff

Die Bedienung der Anwendung erfolgt durch die User der Unternehmen, welche eine Lohnanalyse durchführen.

3.5 Netzwerksicht

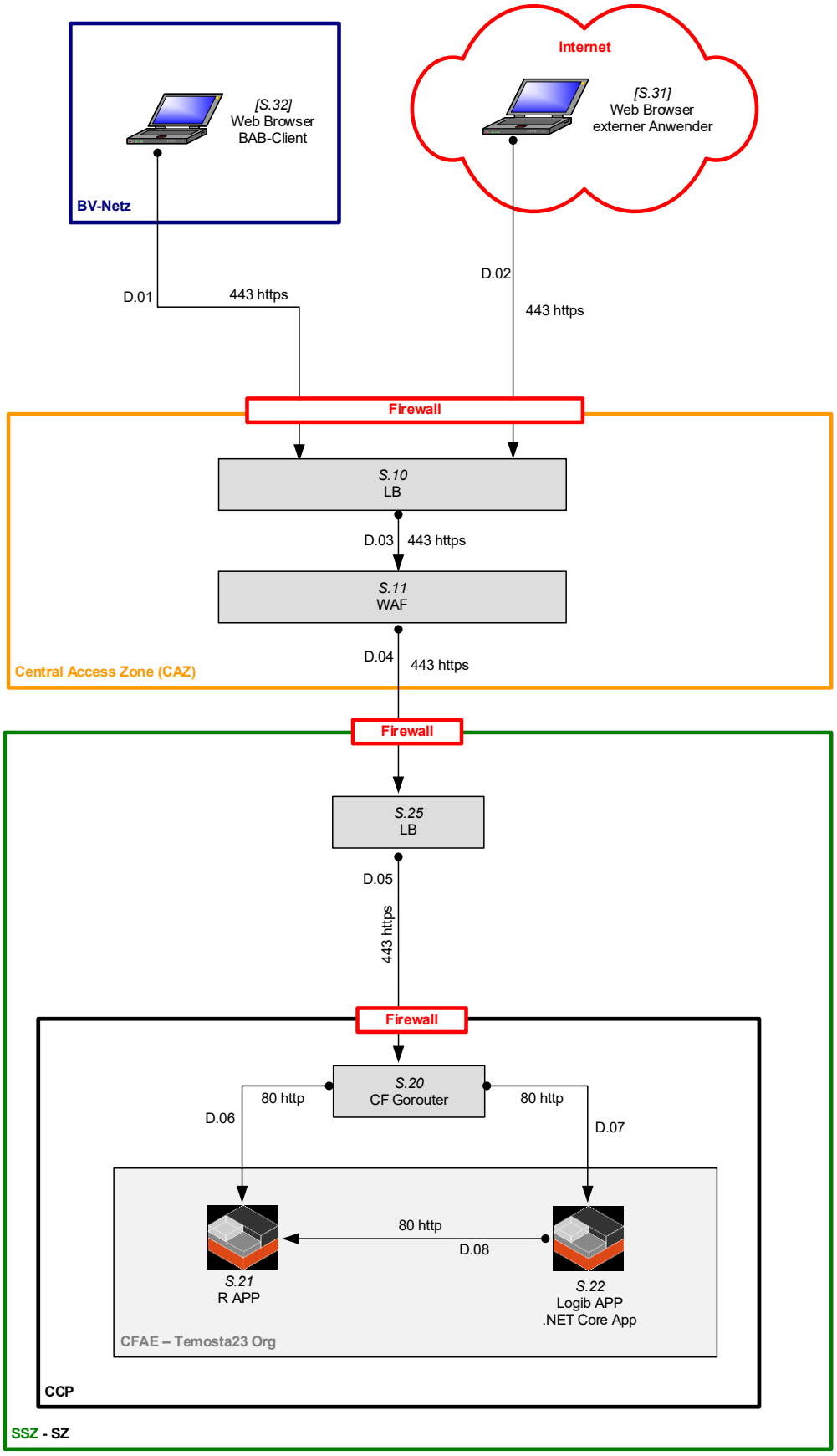

Abbildung 2: Netzw erksicht

4 Vertraulichkeit

4.1 Daten

4.1.1 Was passiert mit den Daten während der Durchführung der Analyse?

1. Die Daten werden lokal im Browser des Anwendenden eingelesen.
2. Um den Browser zu entlasten, wird die Analyse auf dem Server des Bundesamts für Informatik und Telekommunikation durchgeführt. Dafür werden nur zwingend notwendige Informationen über eine verschlüsselte Verbindung übertragen. Bei diesem Vorgang werden keine Daten auf dem Server abgespeichert und es sind keine Rückschlüsse auf das Unternehmen möglich. Weiter gewährleistet dieses Vorgehen, dass auch grosse Datenfiles von Grossbetrieben verarbeitet werden können
3. Die Analyse wird in einen Statistiktool «R» berechnet und nicht im Browser lokal durchgeführt. Der Analyse Code an sich ist nicht trivial. Für dessen Umsetzung ist «R» besser geeignet, als die Javascript Sprachen, welche im Browser verwendet werden.
4. Das Resultat der Lohngleichheitsanalyse wird zurück an den Browser übermittelt.

Der Datenfluss lässt sich wie folgt darstellen, eine besser lesbare Darstellung befindet sich im Anhang, Kap. 11:

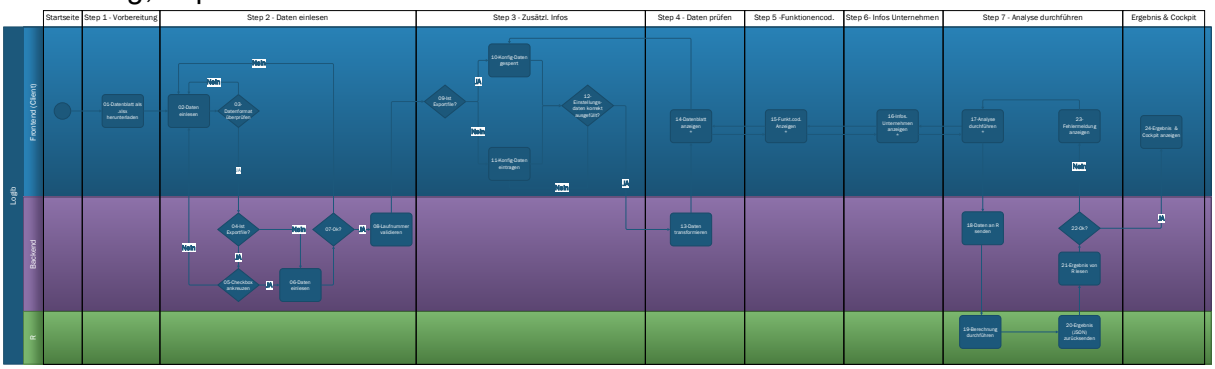

Abbildung 3: Datenfluss Logib

4.1.2 Datenfluss

Die Erklärung zum Datenfluss lautet wie folgt:

Step 1 – Vorbereitung und Vorgehen	01 – Datenblatt als .xlsx herunterladen	Die Userin oder der User kann das Datenblatt als Excel-File für herunterladen.
Step 2 – Daten einlesen	02 – Daten einlesen	Das vom Unternehmen ausgefüllte Datenblatt wird in Logib eingelesen.
	03 – Datenformat überprüfen	Das Format des Datenblatts wird überprüft.
	04 – ist Exportfile?	Ist das Datenblatt ein Exportfile? JA / NEIN

	05 – Checkbox ankreuzen	Wenn es ein Exportfile ist, dann wird die Checkbox angekreuzt.
	06 – Daten einlesen	Die Daten werden im Backend eingelesen.
	07 – ok?	War der Vorgang «Daten einlesen» erfolgreich? JA / NEIN
	08 – Laufnummer validieren	Die Laufnummer wird validiert [→ die Daten werden ans Backend gesandt und auf Doubletten geprüft]
Step 3 – zusätzliche Informationen	09 – Ist Exportfile?	Ist das Datenblatt ein Exportfile? JA / NEIN
	10 – Konfig. Daten gesperrt	Es können keine Konfigurationsdaten im Step 3 ausgefüllt resp. eingetragen werden.
	11 – Konfig. Daten eintragen	Konfigurationsdaten müssen eingetragen werden.
	12 – Einstellungsdaten korrekt ausgefüllt?	Sind die Einstellungsdaten resp. die Konfigurationsdaten richtig ausgefüllt? JA / NEIN
Step 4 – Datenblatt prüfen	13 – Daten transformieren	Die Daten des Datenblatts werden transformiert.
	14 – Datenblatt anzeigen	Das Datenblatt wird angezeigt.
Step 5 – Funktionencodierung bestätigen	15 – Funkt.cod. anzeigen	Die Funkionencodierung wird angezeigt (die Funktionen von 'Daten prüfen' werden übernommen).
Step 6 – Informationen zum Unternehmen	16 – Infos. Unternehmen anzeigen	Optional können Informationen zum Unternehmen angegeben werden.
Step 7 – Analyse durchführen	17 – Analyse durchführen	Die Analyse wird durchgeführt.
	18 – Daten an R senden	Nur die benötigten Daten werden an R gesendet.
	19 – Berechnung durchführen	Die Berechnung wird in R durchgeführt.
	20 – Ergebnis (JSON) zurücksenden	Das Ergebnis wird an den Server zurückgeschickt.
	21 – Ergebnis von R lesen	Das Ergebnis wird vom Server gelesen.

	22 – OK?	Ist das Ergebnis OK? JA / NEIN
	23 – Fehlermeldung anzeigen	Wenn das Ergebnis nicht ok ist, dann wird die Fehlermeldung angezeigt.
Ergebnis & Cockpit	24 – Ergebnis & Cockpit anzeigen[1]	Wenn das Ergebnis ok ist, dann werden das Ergebnis der Analyse und das Cockpit dem User / der Userin angezeigt.

Tabelle 1: Erklärung des Datenflusses Logib

Hinweis: Alle mit «*» gekennzeichneten Steps (d.h. Nr. 14, 15, 16, 17) können nach der durchgeführten Analyse im Modus «Read Only» angeschaut werden.

4.1.3 Werden die Daten gespeichert?

Es werden keine Daten permanent gespeichert. Siehe auch Punkt 4.3.

4.1.4 Werden die Daten weiterverarbeitet?

Die Daten werden nicht durch Dritte weiterverarbeitet.

4.1.5 Wie wird die Datensicherheit garantiert?

Die Datensicherheit hat drei Eckpfeiler:

1. Gesicherte Verbindung

   Die Daten werden über eine TLS-verschlüsselte Verbindung übertragen.

   TLS (Transport Layer Security) ist ein Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet.

2. Anonyme Daten (es werden keine Namen, Vornamen und Funktionsnamen übermittelt).

   Die übermittelten Daten sind anonymisiert und daher nicht kritisch, was den Inhalt betrifft.

   Voraussetzung dafür ist die korrekte Aufbereitung der vom User eingelesenen Daten. Wenn fälschlicherweise Namen und Vornamen im Datensatz enthalten sind, werden auch personalisierte Daten verarbeitet. Daher gilt es, auf die Anonymisierung gemäss Wegleitung zu achten.

   Die Anwendung Logib kann die Erstellung der durch die User eingelieferten Daten nicht beeinflussen.

3. Keine Datenspeicherung

   Die Daten werden nicht gespeichert, sondern sind nur in der laufenden Session verfügbar.

[1] Templates werden vom Frontend an das Backend gesandt und dort mit den entsprechenden Daten gefüllt → openxml füllt die Variablen der Templates aus.

4.1.6 Sind die Daten einsehbar?

Die Daten können nur von der anwendenden Person selbst eingesehen werden. Die generierten Dokumente werden nirgends abgelegt und nicht an Dritte weitergeleitet. Sie können während der laufenden Session durch den oder die Anwendende/n heruntergeladen werden.

4.2 Datenübertragung

4.2.1 Verschlüsselung

Die Datenübertragung erfolgt via TLS verschlüsselt über https.

4.3 Löschung der Daten

4.3.1 Wie werden die Daten gelöscht?

Sobald der Web-Browser geschlossen wird, sind auch die eingelesenen Daten gelöscht. Daher besteht keine Möglichkeit, den Browser vorübergehend zu schliessen und später wieder auf die zuvor eingelesenen Daten bzw. auf deren Auswertung zu zugreifen. Der User hat jederzeit die Möglichkeit, die lokal im Browser Cache gespeicherten Daten über die Funktion «Export Datenblatt als Excel-Datei» lokal abzuspeichern um zu einem späteren Zeitpunkt wieder in Logib einzulesen und mit der Analyse weiterzufahren.

4.4 Personendaten

4.4.1 Werden Personendaten in die Web-Applikation eingelesen?

Es wird eine Datei, das Datenblatt als Excel-Vorlage, mit allen Mitarbeitern in den lokalen Browser Cache eingelesen. Für die Analyse zwingend sind: Referenzmonat, -jahr, Laufnummer, Alter, Geschlecht, Dienstjahre, Ausbildung, Funktion, Betriebliches Kompetenzniveau, Berufliche Stellung, Beschäftigungsgrad oder bezahlte Stunden sowie die einzelnen Lohnbestandteile. Es können weitere Angaben, wie Name, AHV-Nummer, Adresse zu einzelnen Personen eingetragen werden. Dies wird jedoch nicht empfohlen, damit die Vertraulichkeit gewährleistet ist.

Für die Analyse werden nur die notwendigen Daten an den R-Server (vgl. Punkt 4.1.1) übermittelt:

- Die Laufnummer wird anonymisiert
- Die Funktion wird für die Analyse nicht benötigt und ist ausschliesslich im lokalen Cache des Browsers gespeichert

Während der Analyse bleiben die Personendaten im offenen Browser ersichtlich, sobald dieser jedoch geschlossen wird, werden die eingelesenen Daten gelöscht.

Im Wizard Step «Informationen zum Unternehmen» können optional Angaben zum Unternehmen, wie bsp. Firmenname, Adresse, Kontaktperson, Telefon und Email, angegeben werden. Diese Informationen werden, sofern genutzt, ebenfalls an das Backend weiter geleitet und in den Ergebnisdokumenten sowie in die Exportfiles (z.B. Excel) abgefüllt[2].

[2] Templates werden vom Frontend an das Backend gesandt und dort mit den entsprechenden Daten gefüllt, → openxml füllt die Variablen der Templates aus.

4.4.2 Was passiert mit den Personendaten?

Diese werden für die Berechnung der Lohngleichheit ans Backend geschickt und dort so lange im Memory gehalten, wie sie für die jeweils laufende Analyse gebraucht werden. Die Daten werden aktuell nicht persistiert. Siehe detailliertere Erklärung Punkt 4.1.1.

4.5 Klassifizierte Informationen

4.5.1 Werden klassifizierte Informationen nach ISchV bearbeitet?

Gemäss der Schutzbedarfsanalyse TEMOSTA23 V.1.1, werden keine gemäss ISchV klassifizierten Daten / Informationen durch das System gespeichert, bearbeitet oder ausgewertet.

4.5.2 Werden Informationen, die aus einer speziellen Gesetzgebung besonders geschützt werden müssen, in der Web-Applikation bearbeitet?

Gemäss der Schutzbedafsanalyse TEMOSTA23 V.1.1 werden keine besonders schützenswerten Daten durch das System gespeichert, bearbeitet oder ausgewertet.

5 Verfügbarkeit der Applikation

5.1 Ausfalldauer

5.1.1 Wie lange darf die max. zulässige Ausfalldauer sein?

Die Ausfalldauer kann bis zu maximal 12 Stunden – gemäss Servicekatalog: Verfügbarkeitsklasse 1 – betragen.

5.2 Servicezeiten

5.2.1 Wie sind die Servicezeiten?

Die Servicezeit sind von Montag bis Freitag zwischen 07:00 und 18:00 Uhr.

5.3 IT Service Continuity Management (ITSCM)

5.3.1 Ist der ITSCM relevant als Teil des Business Continuity Management (BCM) für geschäftskritische Prozesse?

Der ITSCM ist nicht relevant als Teil der BCM. Im Notfall besteht die gesamte Webseite vorrübergehend nicht mehr. Für diesen Fall werden organisatorische Massnahmen erarbeitet, wie beispielsweise die kurzfristige Bereitstellung von Logib mit einer anderen Technologie. Dies unter Beibehaltung der bestehenden Sicherheitsstandards.

6 Integrität

6.1 Muss die Echtheit, Korrektheit oder Unversehrtheit der Daten nachgewiesen werden können?

Gemäss der Schutzbedarfsanalyse gibt es betreffend Integrität keine speziellen Anforderungen.
Da die Anwendung online bedient wird und das Ergebnis der Analyse nur an den Datenübermittler zurückgegeben wird, muss keine Funktionalität implementiert werden, die erkennt, ob die Daten unterwegs manipuliert wurden.

7 Nachvollziehbarkeit

7.1 Müssen bestimmte Arbeitsvorgänge nachgewiesen werden können?

Gemäss der Schutzbedarfsanalyse des Bundes gibt es betreffend Nachvollziehbarkeit keine speziellen Anforderungen.
Im Kapitel 9 wird beschrieben, welche Daten in Logfiles gespeichert und wo diese abgelegt werden.

8 RINA-Relevanz

8.1 Ist Logib durch nachrichtendienstliche Ausspähung erheblich gefährdet?

Die Untersuchung in der Schutzbedarfsanalyse hat ergeben, dass Logib nicht RINA relevant ist und keine Gefahr einer nachrichtendienstlichen Ausspähung besteht.

9 Logfiles

9.1 Was ist ein Logfile?

Im IT-Betrieb werden standardisierte Logfiles als Basis für die Wahrnehmung der betrieblichen Aufgaben erstellt. Der IT-Betrieb wird seitens des BIT, organisatorisch und räumlich vom EBG gewährleistet. Somit unterliegen sie den Sicherheitskonventionen des BIT.
Logib schreibt kein Logfile im eigentlichen Sinne. Die Cloud-Foundry-Container loggen auf die entsprechende Konsole. Diese Logs werden von der Containerplattform für eine gewisse Zeit persistiert und können vom Entwicklerteam abgefragt werden.

9.2 Für welchen Zweck werden die Logfiles benutzt?

Die Cloud-Foundry-Plattform als technische Basis hat diverse Schutzfunktionen vor Cyber Angriffen auf die Bundesinfrastruktur. Hierfür werden unter anderem die IP-Adressen der User geloggt. Diese Angaben werden aus Sicherheitsgründen seitens des BIT nicht an andere Teams kommuniziert. Entsprechend gelangen diese Angaben auch nicht an Logib bzw. das Team, welches den IT-Betrieb von Logib gewährleistet bzw. Logib weiter entwickelt.

Die Logs für die Applikation Logib werden für die Analyse von allfälligen durch die User gemeldeten Fehlern benötigt. In den Logs werden nur technische Details des aufgetretenen Fehlers verknüpft und mit einer Request ID ausgegeben. Dies erlaubt nachzuvollziehen, wo während eines Prozesses mehrere verschiedene Fehler aufgetreten sind. Ein Rückschluss auf den Nutzer ist nicht möglich. Hierfür werden folgende Daten pro Session des Frontend, Logib, temporär gelogged: Datum, Uhrzeit, Anstoss der 1. Analyse im Wizard und Informationen zu Fehlern/Warnings. Nutzerdaten werden in den Logs nicht gespeichert.

Darüber hinaus, getrennt vom Frontend, erkennt die Cloud-Foundry-Plattform wie beschrieben die IP-Adresse.

9.3 Wo werden die Logfiles gespeichert?

Die Logfiles werden auf der Cloud-Foundry-Plattform gespeichert. Diese wird durch das CCP-Team des BIT unterhalten. Das CCP-Team ist organisatorisch in einem separaten Bereich aufgestellt.

9.4 Wie werden die Logfiles gelöscht?

Die Logs auf der Cloud-Foundry-Plattform werden aus Gründen der Sicherheit 90 Tage behalten. Im Anschluss werden sie automatisch durch die Plattform selbst gelöscht.
Dies kann auf der Plattform konfiguriert werden.

9.5 Wie wird die Datensicherheit der Logfiles gewährleistet?

Die Cloud Foundry Plattform wird durch das BIT bereitgestellt und betrieben. Die Verantwortung für die Sicherheit der Logs liegt daher beim CCP-Team des BIT. Zugriffe sind gemäss Sicherheits [ISDS-]- und Zugriffskonzept für das CCP-Team geregelt.

10 Analysefehler

Tritt im Verlauf der Nutzung von Logib ein Fehler auf, wird dem Nutzer eine entsprechende Fehlermeldung in Form einer Oblique Notification angezeigt und die technischen Details des Fehlers werden gemäss Kapitel 9 in ein Log ausgegeben.

11 Anhang

11.1 Grafik zum Datenfluss Logib

Nachfolgend ist die Grafik zum Datenfluss von Logib ersichtlich:

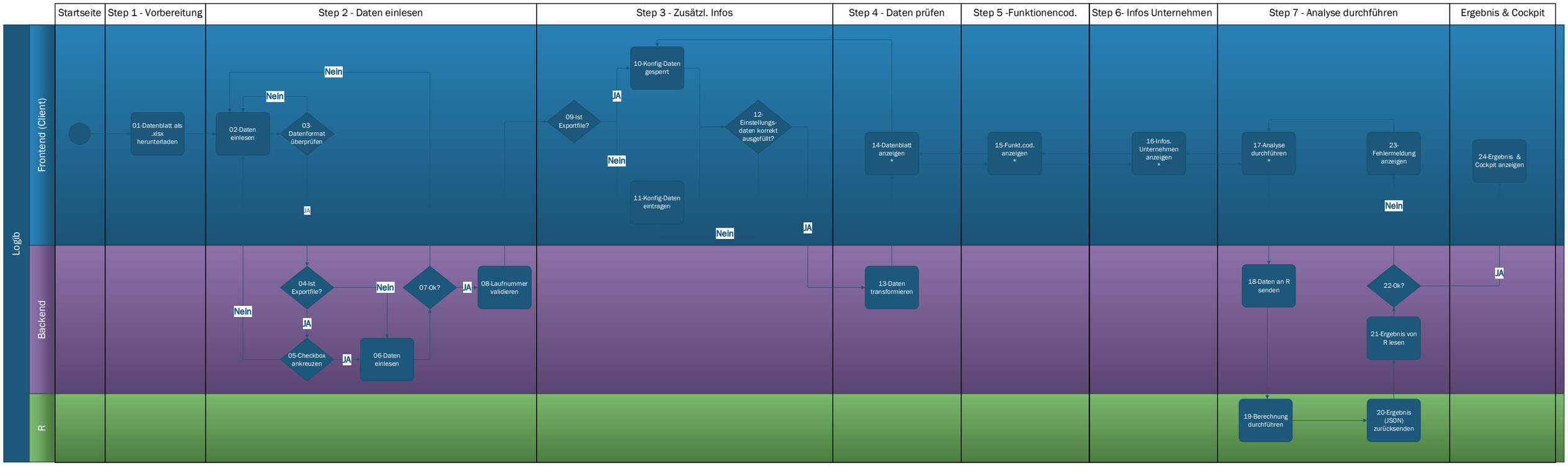

Abbildung 4: Datenfluss Logib [vergrössert]

12 Glossar

Begriff / Abkürzung	Bedeutung
.NET Core 3.x	Eine freie und quelloffene Software Plattform der :NET Plattform, die zur Entwicklung und Ausführung von Anwendungsprogrammen dient und unter der Koordination von Microsoft entwickelt wird.
BCM	Business Continuity Management
Beschaffungswesen	Nach Art. 8 Abs. 1 Bst. c BöB [6]
BIT	Bundesamt für Informatik und Telekommunikation [7]
BV-Netz	Das Netz der Bundesverwaltung.
CAZ	Central Access Zone resp. die zentrale Zugriffszone.
Cloud Foundry	Die strategische Cloud-Kubernetes-Plattform des BIT.
Container	Container sind ein aktueller Trend in der IT. Sie verpacken eine Anwendung und alle zu ihrer Ausführung erforderlichen Dateien in ein handliches Paket.
EBG	Eidgenössische Büro für die Gleichstellung von Frau und Mann [8]
GIG	Gleichstellungsgesetz.
HTTPS	Hyptertext Transfer Protocol Secure ist ein Kommunikationsprotokoll im World Wide Web, welches eine Transportverschlüsselung darstellt, d.h. Daten werden abhörsicher übertragen.
ISchV	Informationsschutzverordnung Bund [9]
ITSCM	IT Service Continuity Management
JavaScript	JavaScript ist eine Skriptsprache, die ursprünglich für dynamisches HTML in Webbrowsern entwickelt wurde.
JSON	Die JavaScript Object Notation (JSON) ist ein kompaktes Datenformat in einer einfach lesbaren Textform und dient dem Zweck des Datenaustausches zwischen Anwendungen.

Begriff / Abkürzung	Bedeutung
LB	Load Balancer ist ein Lastverteiler in einer Server-Infrastruktur.
Logfile	Eine Logdatei enthält automatisch geführte Protokolle aller oder einer bestimmter Aktion von Prozessen auf einem Computersystem.
Logib	Standard-Analyse-Tool des Bundes für Lohngleichheitsanalysen.
Matomo	Ein kostenloses Analyse-Probramm.
Oblique / Angular	Ein Frontend Framework für Schweizer UI-Marken.
Plumber (REST API)	Plumber ermöglicht es, eine WEB-Anwendungsschnittstelle (API) zu erstellen, welche die Kommunikation zwischen Backend und R sicherstellt.
R	Open-Source-Programm(iersprache) für statistische Berechnungen und Grafiken.
RINA	RINA (Risikomanagementmethode zur Reduktion nachrichtendienstlicher Ausspähung des ISB) ist ein Prüfprozess.
Schuban	Schutzbedarfsanalyse [3]
SSZ	Shared Service Zone
SZ	Server Zone
TLS	Transport Layer Security, auch bekannt als Secure Sockets Layer (SSL), ist ein hybrides Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet.
UI	User Interface (UI) ist der englische Begriff für Benutzeroberflächen oder Benutzerschnittstellen, der die Art und Weise beschreibt, mit der ein Anwender mit einer Maschine in Kontakt tritt.
WAF	Web Application Firewall ist ein Verfahren, welches Webanwendungen vor Angriffen über das http schützen soll.

Tabelle 2: Glossar

13 Referenzen

[1] Eidgenössische Büro für die Gleichstellung von Frau und Mann, „Lohngleichheit analysieren - einfach und sicher mit Logib,“ [Online]. Available: www.logib.ch. [Zugriff am 26 06 2020].

[2] Eidgenössische Büro für die Gleichstellung von Frau und Mann (EBG), „Häufige Fragen zur Lohngleichheitsanalyse nach Gleichgestellungsgesetz (GIG),“ [Online]. Available: https://www.ebg.admin.ch/ebg/de/home/themen/arbeit/lohngleichheit/lohngleichheitsanalyse-gleichstellungsgesetz.html#2035398151. [Zugriff am 26 06 2020].

[3] Informatiksteuerungsorgan des Bundes (ISB), „PO41 - Schutzbedarfsanaylse (Schuban),“ 28 01 2020. [Online]. Available: https://www.isb.admin.ch/isb/de/home/ikt-vorgaben/prozesse-methoden/p041-schutzbedarfsanalyse_schuban.html. [Zugriff am 26 06 2020].

[4] Informatiksteuerungsorgan des Bundes (ISB), „Si001 - IKT-Grundschutz in der Bundesverwaltung,“ 22 12 2019. [Online]. Available: https://www.isb.admin.ch/isb/de/home/ikt-vorgaben/sicherheit/si001-ikt-grundschutz_in_der_bundesverwaltung.html. [Zugriff am 26 06 2020].

[5] Eidgenössische Büro für die Gleichstellung von Frau und Mann (EBG), „Konformitätserklärung Logib,“ 18 03 2020. [Online]. Available: https://www.ebg.admin.ch/dam/ebg/de/dokumente/lohngleichheit/logib/konformitaetserklaerung_logib.pdf.download.pdf/Konformit%C3%A4tserkl%C3%A4rung_Standard-Analyse-Tool%20(Logib)_V2020.1.pdf. [Zugriff am 26 06 2020].

[6] Der Bundesrat, „172.056.1 - Bundesgesetz über das öffentliche Beschaffungswesen (BöB),“ 20 06 2020. [Online]. Available: https://www.admin.ch/opc/de/classified-compilation/19940432/index.html. [Zugriff am 26 06 2020].

[7] Bundesamt für Informatik und Telekommunikation (BIT), „Home,“ [Online]. Available: https://www.bit.admin.ch/bit/de/home.html. [Zugriff am 26 06 2020].

[8] Eidgenössische Büro für die Gleichstellung von Frau und Mann (EBG), „Home,“ [Online]. Available: https://www.ebg.admin.ch/ebg/de/home.html. [Zugriff am 26 06 2020].

[9] Der Bundesrat, „Verordnung über den Schutz von Informationen des Bundes,“ 01 01 2018. [Online]. Available: https://www.admin.ch/opc/de/classified-compilation/20070574/index.html. [Zugriff am 03 07 2020].