Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Home Affairs FDHA

Federal Office for Gender Equality (FOGE)

Security Declaration

Standard Analysis Tool (Logib)
Security verification

1 Context

In accordance with Art. 13*c* para. 2 of the Gender Equality Act (GEA) the Confederation provides employers with a free standard tool for conducting wage equality analyses. With this declaration of conformity, employers who conduct wage equality analyses as per Art. 13*a* GEA with the standard analysis tool can provide verification of a scientifically rigorous and legally compliant method in accordance with Art. 13*c* para. 1 GEA (see Art. 7 para. 3 Ordinance on the evaluation of the wage equality analysis). The standard analysis tool (Logib) was developed by the Federal Office for Gender Equality (FOGE) with the support of private specialist institutions in the early 2000s. The Federal Office of Information Technology, Systems and Telecommunication (FOITT) has been operating Logib as a web application through FOGE since 2020.

1.1 Security verification

As stipulated in the security specifications (IT Basic Protection), a security requirements analysis and IT Basic Protection specification were created and put into effect. The security measures are transparently and comprehensively set out in the Appendix.

The Federal Office for Gender Equality FOGE hereby confirms that the standard analysis tool (Logib) meets all of the Confederation's security specifications as per the security requirements specification and the IT Basic Protection specification. The web application does not process any sensitive data. The web application is updated regularly and checked for security loopholes.

Bern, October 2020

Durrer Sylvie 0GP82L
Signature numérique de Durrer Sylvie 0GP82L
Date : 2020.10.21 09:37:59 +02'00'

Digital signiert von Grossenbacher Markus RIXGTO
2020-10-20 (mit Zeitstempel)

Aeberhard Patric PURVAM
Digital unterschrieben von Aeberhard Patric PURVAM
Datum: 2020.10.20 08:14:34 +02'00'

Sylvie Durrer	**Markus Grossenbacher**	**Patric Aeberhard**
Director FOGE	Chief Security Officer FOITT	Wage equality expert FOGE

Appendix of Security Declaration

Status	In progress, under review, approved
Version	2020.2

Contents

List of figures

List of tables

2 Introduction to the Security Declaration

This document provides an overview of the security measures that are applied to the standard analysis tool (Logib). They are described in detail in a question and answer format from Section 3.1 onwards.

2.1 What is Logib?

Logib [1] is the Confederation's standard analysis tool for assessing equal pay practices.

The Federal Office for Gender Equality (FOGE) enhanced Logib in collaboration with the Federal Office of Information Technology, Systems and Telecommunication (FOITT) so that employers could, on the one hand, perform a self-test to review their pay practice for compliance with the gender-based equal pay requirement and, on the other hand, perform compliance checks in their procurement processes (Art. 8 para. 1 (c) PPA).

2.2 The revised Gender Equality Act: Art. 13*a* et seq. GEA

The revised Gender Equality Act (GEA) entered into force on 1 July 2020, requiring companies with 100 or more employees to conduct an equal pay analysis every four years and have it verified by an independent body. Furthermore, the employees and shareholders must be informed of the result of the wage equality analysis. According to Art. 13*c* para. 2 GEA, the Confederation is moreover obliged to provide all employers with a free standard analysis tool. At the same time, an ordinance was put into effect that regulates the training of the auditing companies, the evaluation of the wage equality analyses as well as the schedule [2].

2.3 Verification of security

As stipulated in the security specifications (IT Basic Protection), a security requirements analysis [3] and IT Basic Protection specification [4] were created and put into effect.

2.4 Brief description of the Security Declaration

The main points of this Security Declaration are briefly listed below:

- The data is only available to the user during the current browser session and is therefore not permanently stored anywhere.
- The data can only be edited locally in the user's browser cache. Third parties therefore have no access to it.
- All data is deleted once the browser is closed.
- The data is transmitted using https, i.e. in encrypted form.
- The Logib server is operated by the Federal Office of Information Technology, Systems and Telecommunication.
- The Logib application is based on scientifically rigorous and legally compliant methods [5].

3 Architecture

This section outlines the architecture and its technical implementation.

3.1 Logib overview

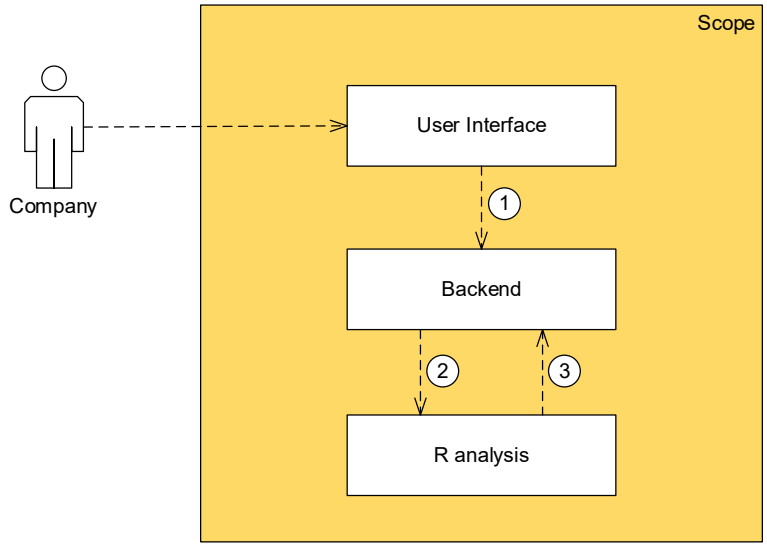


Figure 1: Logib overview

3.2 What is the technical basis of Logib?

3.2.1 User interface

This component allows the user to interact with the system.

In the current system (phase 2), the user does not need to log in.

- Plausibility check on the data submitted (except validation of sequential number)
- Syntax check on the data submitted
  →https://confluence.bit.admin.ch/pages/viewpage.action?pageId=268097910
- Graphical representation of the data from the analysis component (R) using JavaScript Highcharts software library.

Product/technology

The frontend framework is Oblique/Angular.

The user interface and backend elements are implemented together in the form of a microservice.

3.2.2 Backend

The backend module primarily performs the following functions:

- Read the data file and convert into a JSON file
- Convert age, gender, years of service
- Validate the sequential number (not on UI for performance reasons)
- Send the data to R in JSON format and receive it from R in JSON format

Product/technology

.NET Core 3.x

→Free open-source software platform on the .NET platform for developing and running applications, developed with the coordination of Microsoft.

The user interface and backend elements are implemented together in the form of a microservice and are located in the same container.

3.2.3 R analysis

The R analysis component as the backend deals purely with the calculations (basis for wage standardisation, regressions analysis, cockpit figures). It does not prepare any diagrams, tables, etc.

The backend transfers the data in the form of a JSON file.

The results of the calculations are sent back to the backend, also in the form of JSON.

For details of the attributes, please refer to the detailed interface description in Section 4.1.2 Data flow.

Products/technology:

- Plumber (REST API) for communication between the backend and R analysis components.
- The R analysis component is implemented in its own container.

3.3 Where are the servers located?

The servers are located in the protected computer centres of the Federal Office of Information Technology, Systems and Telecommunication in Switzerland.

3.4 How can Logib be accessed?

3.4.1 Internal access

It is unavoidable that systems administrators as well as developers and testers of the application have access to the application through a personalised user role.

3.4.2 External access

The application is used by the users in the companies that conduct a wage analysis.

3.5 Network view

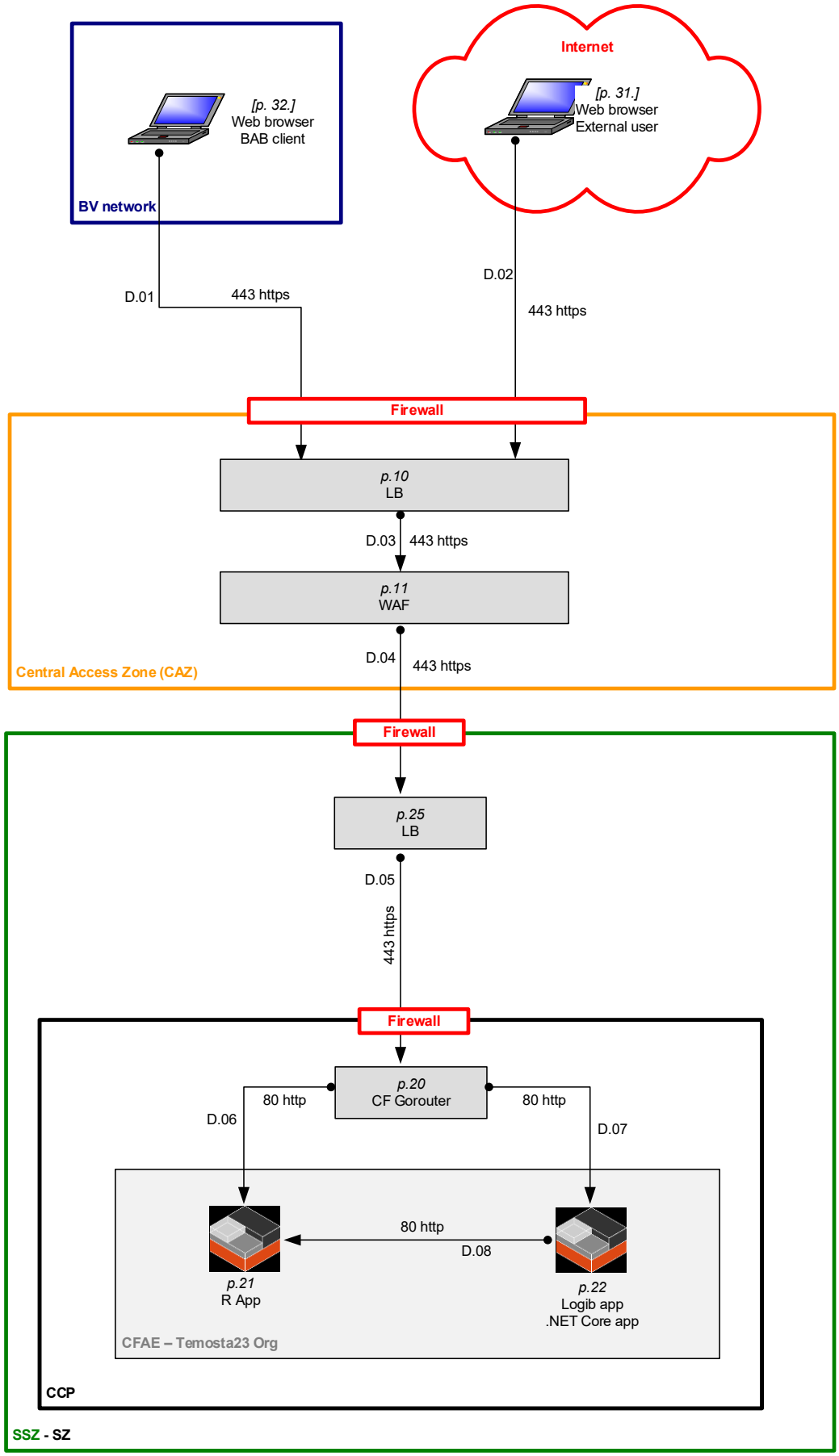


Figure 2: Network view

4 Confidentiality

4.1 Data

4.1.1 What happens to the data during the analysis?

1. The data is imported locally in the user's browser.
2. To relieve the browser's workload, the analysis is performed on the server of the Federal Office of Information Technology, Systems and Telecommunication. Only the information that is absolutely necessary is transmitted through an encrypted connection. No data is saved on the server during this process, and it is not possible to identify a company from the data. This arrangement ensures that the large data files of major companies can also be processed.
3. The analysis is calculated in an "R" statistics tool and not performed locally in the browser. The analysis code itself is not trivial. "R" is more suitable for its implementation than the Javascript languages used in browsers.
4. The result of the wage equality analysis is sent back to the browser.

The data flow can be illustrated as follows. For a more legible version of the diagram please refer to the Appendix in Section 11:

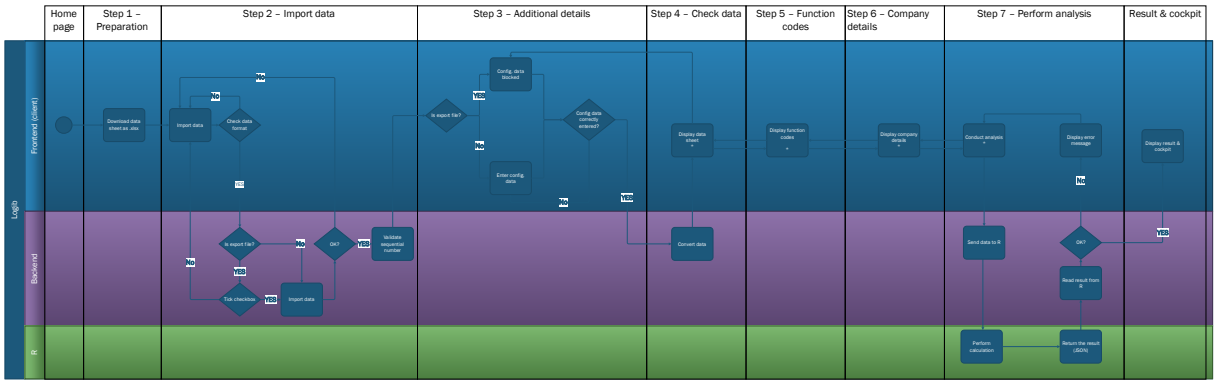


Figure 3: Logib data flow

4.1.2 Data flow

The explanation of the data flow is as follows:

Step 1 – Preparation and process	01 – Download data sheet in .xlsx format	The user can download the data sheet as an Excel file.
Step 2 – Import data	02 – Import data	The data sheet that was completed by the company is imported into Logib.
	03 – Check data format	The format of the data sheet is checked.
	04 – Is it an export file?	Is the data sheet an export file? YES/NO
	05 – Tick checkbox	If it is an export file, the checkbox is ticked.

	06 – Import data	The data is imported into the backend.
	07 – OK?	Was the "Import data" step successful? YES/NO
	08 – Validate sequential number	The sequential number is validated [→ the data is sent to the backend and checked for duplicates]
Step 3 – Additional information	09 – Is it an export file?	Is the data sheet an export file? YES/NO
	10 – Config. data blocked	No configuration data can be entered in Step 3.
	11 – Enter config. data	Configuration data must be entered.
	12 – Settings data correctly entered?	Was the configuration data or settings data entered correctly? YES/NO
Step 4 – Check data sheet	13 – Convert data	The data in the data sheet is converted.
	14 – Display data sheet	The data sheet is displayed.
Step 5 – Confirm function codes	15 – Display function codes	The function codes are displayed (the functions from 'Check data' are used).
Step 6 – Information about the company	16 – Display company details	Optional information about the company can be entered.
Step 7 – Perform analysis	17 – Perform analysis	The analysis is performed.
	18 – Send data to R	Only the required data is sent to R.
	19 – Perform calculation	The calculation is done in R.
	20 – Return the result (JSON)	The result is sent back to the server.
	21 – Read the result from R	The server reads the result.
	22 – OK?	Is the result OK? YES/NO
	23 – Display error message	If the result is not ok, the error message is displayed.
Result & cockpit	24 – Display result & cockpit[1]	If the result is ok, the result of the analysis and the cockpit are displayed to the user.

Table 1: Explanation of Logib data flow

Note: All steps marked with "*" (i.e. 14, 15, 16, 17) can be viewed in "read only" mode once the analysis has been completed.

[1] Templates are sent from the frontend to the backend and then completed with data there → openxml fills in the template variables.

4.1.3 Is the data stored?

No data is permanently stored. See also Section 4.3.

4.1.4 Is the data processed further?

The data is not processed by third parties.

4.1.5 How is data security ensured?

Data security has three cornerstones:

1. Secure connection

   The data is transferred via a TLS encrypted connection.

   TLS (Transport Layer Security) is an encryption protocol for secure data transmission over the Internet.

2. Anonymous data (no last names, first names or function names are transmitted).

   The transmitted data is anonymised and therefore not critical in terms of content.

   This requires that the data imported by the user is correctly prepared. If any last names or first names are mistakenly included in the record, personalised data will also be processed. It is therefore important to make sure that the data is anonymised as described in the guideline.

   The Logib application has no influence over the way the data sent by the users is created.

3. No data storage

   The data is not stored. It is only available in the current session.

4.1.6 Can the data be viewed by others?

The data can only be viewed by the user of the application. The generated documents are not stored anywhere and they are not forwarded to any third parties. They can only be downloaded by the user during the current session.

4.2 Data transmission

4.2.1 Encryption

Data transmissions are TLS-encrypted using https.

4.3 Deletion of data

4.3.1 How is the data deleted?

As soon as the web browser is closed, the imported data is deleted. It is therefore not possible to close the browser temporarily and later access the data that was previously imported, or its analysis. The user can save the data stored locally in the browser cache to the local drive at any time with the "Export data sheet as Excel file" function and import it back into Logib later to continue with the analysis.

4.4 Personal data

4.4.1 Is any personal data imported into the web application?

One file, the data sheet that contains all the employees, based on the Excel template, is imported into the local browser's cache. The following information is required for the analysis: reference month and year, sequential number, age, gender, length of service, training, function, occupational skill level, professional position, activity rate or paid hours and the individual wage components. It is possible to enter further details, such as name, AHV number, or address of the individual persons. To ensure confidentiality, however, this is not recommended.

Only the required data is transferred to the R server for the analysis (see Section 4.1.1):

- The sequential number is anonymised
- The function is not required for the analysis and is only saved in the browser's local cache.

During the analysis, the personal data remains visible in the open browser, however as soon as the browser is closed, the data that was imported is deleted.

In the wizard step "Information about the company", optional details about the company can be entered, such as company name, address, contact person, telephone and e-mail address. This information, if used, is also sent to the backend and included in the results documents as well as the export files (e.g. Excel)[2].

4.4.2 What happens to the personal data?

Personal data is sent to the backend for the wage equality calculation and kept in the memory there for as long as it is required for the current analysis. At present, this data is not persisted. See Section 4.1.1 for a detailed explanation.

4.5 Classified information

4.5.1 Is classified information processed in accordance with the IPO?

According to the security requirements analysis for TEMOSTA23 v1.1, no data/information classified in accordance with the IPO (Ordinance on the Protection of Federal Information) is stored, processed or evaluated by the system.

4.5.2 Does the web application process any information that needs extra protection under special legislation?

According to the security requirements analysis for TEMOSTA23 v1.1, no sensitive data is stored, processed or evaluated by the system.

[2] Templates are sent from the frontend to the backend and then completed with data there → openxml completes the template variables.

5 Availability of the application

5.1 System outages

5.1.1 How long is the max. permissible duration of system unavailability?

In line with availability class 1 in the service catalogue, system outages may not exceed 12 hours.

5.2 Service times

5.2.1 What are the service times?

The service times are Monday to Friday from 7 a.m. to 6 p.m.

5.3 IT Service Continuity Management (ITSCM)

5.3.1 Is ITSCM relevant as part of Business Continuity Management (BCM) for business-critical processes?

ITSCM is not relevant as part of BCM. In an emergency, the entire website is temporarily unavailable. In this case, organisational measures are developed, such as the temporary provision of Logib with a different technology. This while maintaining the existing safety standards.

6 Integrity

6.1 Does the authenticity, correctness or integrity of the data need to be verifiable?

According to the security requirements analysis, there are no special requirements concerning integrity.
Because the application is used online and the result of the analysis is only returned to the person who sent the data, no functionality needs to be implemented to determine if the data was manipulated in transit.

7 Traceability

7.1 Do certain work processes need to be verifiable?

According to the federal security requirements analysis, there are no special requirements concerning transparency.
Section 9 describes which data is stored in log files and where these are stored.

8 Relevance of RINA

8.1 Is Logib at significant risk of espionage?

The investigation for the security requirements analysis showed that Logib is not RINA relevant and there is no danger of espionage.

9 Log files

9.1 What is a log file?

In the IT operation, standardised log files are produced as a basis for performing the operational tasks. In technical terms, the IT operation is provided by FOITT and in organisational terms by FOGE, in separate locations. The log files are therefore subject to the FOITT security regulations.
Logib does not write any log files as such. The Cloud Foundry containers connect to the respective consoles. These logs are persisted on the container platform for a certain amount of time and can be queried by the developer team.

9.2 For what purpose are the log files used?

The Cloud Foundry platform which provides the system's technological basis has various functions to protect the federal infrastructure from cyber attacks. This includes logging the IP addresses of the users. For security reasons, FOITT does not communicate these details to other teams. These details therefore do not reach Logib or the team in charge of Logib IT operations or its ongoing development.

The logs for the Logib application are required in order to analyse any errors that users may report. The logs only link the technical details of an error to a request ID. This allows us to trace back where multiple different errors have occurred during a process. It is not possible to conclude the user's identity from these logs. The following data is temporarily logged for each Logib frontend session: date, time, start of the first analysis in the wizard and error/warning information. No user data is stored in the logs.

Furthermore, independently of the frontend, the Cloud Foundry platform recognises the IP address as described.

9.3 Where are the log files stored?

The log files are stored on the Cloud Foundry platform which is maintained by the FOITT's CCP team. In organisational terms, the CCP team is set up in a separate area.

9.4 How are the log files deleted?

For security reasons, the logs on the Cloud Foundry platform are kept for 90 days. After this, the platform automatically deletes them.
This can be configured on the platform.

9.5 How is the data security of the log files ensured?

The Cloud Foundry platform is provided and operated by the FOITT. The responsibility for the security of the logs therefore lies with the FOITT CCP team. Access by the CCP team is regulated in accordance with the security [ISDS] concept and the access concept.

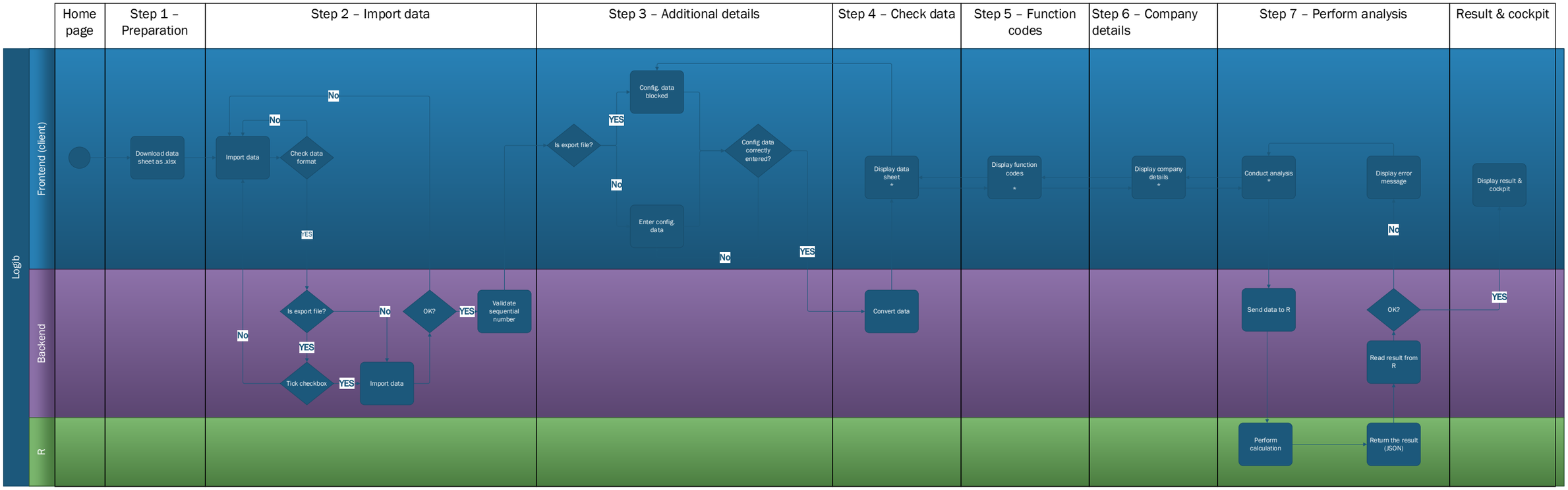
10 Analysis errors

If an error occurs while using Logib, the respective error message is displayed to the user in the form of an Oblique notification and the technical details of the error are written to a log as described in Section 9.

11 Appendix

11.1 Diagram of Logib data flow

Here is the diagram of the Logib data flow:



Note:

* Once the analysis has been performed, the user can view the wizards marked with * in "read only" mode.

Figure 4: Logib data flow [high resolution]

12 Glossary

Term / abbreviation	Meaning
.NET Core 3.x	A free open-source software platform of the .NET platform which serves to develop and run applications and was developed under the coordination of Microsoft.
BCM	Business Continuity Management
Procurement	According to Art. 8 para. 1 (c) PPA [6]
FOITT	Federal Office of Information Technology, Systems and Telecommunication [7]
BV network	The network of the Federal administration.
CAZ	Central Access Zone
Cloud Foundry	The FOITT's strategic Cloud-based Kubernetes platform.
Container	Containers are a current trend in IT. They contain an application and all the files required to run it in a handy package.
FOGE	Federal Office for Gender Equality [8]
GEA	Gender Equality Act
HTTPS	Hypertext Transfer Protocol Secure is an Internet communication protocol that encrypts connections at the transport layer, i.e. the data is transferred in a way that is secure from eavesdropping.
IPO	Federal Information Protection Ordinance [9]
ITSCM	IT Service Continuity Management
JavaScript	JavaScript is a scripting language that was originally developed for dynamic HTML in web browsers.
JSON	JavaScript Object Notation (JSON) is a compact data format in readily legible text form used for exchanging data between applications.
LB	A load balancer distributes the workload in a server infrastructure.

Term / abbreviation	Meaning
Log file	Log files contain automatically recorded logs of all activities or a specific subset of activities of processes on a computer system.
Logib	The Confederation's standard analysis tool for assessing equal pay practices.
Matomo	A free analysis program.
Oblique / Angular	A frontend framework for Swiss UI brands.
Plumber (REST API)	Plumber enables the creation of a web application programming interface (API) to secure communication between the backend and R.
R	Open source program (and programming language) for statistical calculations and diagrams.
RINA	RINA (the Federal IT Steering Unit's risk management method to reduce intelligence spying) is a verification process.
Schuban	Security requirements analysis (Schutzbedarfsanalyse) [3]
SSZ	Shared Service Zone
SZ	Server Zone
TLS	Transport Layer Security, also known as the Secure Sockets Layer (SSL), is a hybrid encryption protocol for secure data transmission on the Internet.
UI	The user interface is the means by which a user interacts with a computer system.
WAF	Web Application Firewall is a process that protects web applications from attacks via http.

Table 2: Glossary

13 References

[1] Federal Office for Gender Equality, "Analyse equal pay - simply and securely with Logib," [Online]. Available: www.logib.ch. [Accessed 26 06 2020].

[2] Federal Office for Gender Equality (FOGE), "Häufige Fragen zur Lohngleichheitsanalyse nach Gleichgestellungsgesetz (GIG) (eng.: Frequently Asked Questions on the wage equality analysis in accordance with the Gender Equality Act)," [Online]. Available: https://www.ebg.admin.ch/ebg/de/home/themen/arbeit/lohngleichheit/lohngleichheitsanalyse-gleichstellungsgesetz.html#2035398151. [Accessed 26 06 2020].

[3] Federal IT Steering Unit (FITSU), "PO41 - Schutzbedarfsanalyse (Schuban) (eng. Security Requirements Analysis)," 28 01 2020. [Online]. Available: https://www.isb.admin.ch/isb/de/home/ikt-vorgaben/prozesse-methoden/p041-schutzbedarfsanalyse_schuban.html. [Accessed 26 06 2020].

[4] Federal IT Steering Unit (FITSU), "Si001 - IT Basic Protection," 22 12 2019. [Online]. Available: https://www.isb.admin.ch/isb/en/home/ikt-vorgaben/sicherheit/si001-ikt-grundschutz_in_der_bundesverwaltung.html. [Accessed 26 06 2020].

[5] Federal Office for Gender Equality (FOGE), "Declaration of conformity," 18 03 2020. [Online]. Available: https://www.ebg.admin.ch/dam/ebg/en/dokumente/lohngleichheit/logib/konformitaetserklaerung_logib.pdf.download.pdf/Konformit%C3%A4tserkl%C3%A4rung_Standard-Analyse-Tool%20(Logib)_V2020.1.pdf. [Accessed 26 06 2020].

[6] The Federal Council, "172.056.1 - Bundesgesetz über das öffentliche Beschaffungswesen (BöB) (eng.: Swiss Federal Law on Government Procurement)," 20 06 2020. [Online]. Available: https://www.admin.ch/opc/de/classified-compilation/19940432/index.html. [Accessed 26 06 2020].

[7] Federal Office of Information Technology, Systems and Telecommunication (FOITT), "Home," [Online]. Available: https://www.bit.admin.ch/bit/en/home.html. [Accessed 26 06 2020].

[8] Federal Office for Gender Equality (FOGE), "Home," [Online]. Available: https://www.ebg.admin.ch/ebg/en/home.html. [Accessed 26 06 2020].

[9] The Federal Council, "Ordinance on the Protection of Federal Information" 01 01 2018. [Online]. Available: https://www.admin.ch/opc/en/classified-compilation/20070574/index.html. [Accessed 03 07 2020].