



Déclaration de sécurité

Outil d'analyse standard (Logib) Preuve concernant la sécurité

1 Contexte

Conformément à l'art. 13c, al. 2 de la loi sur l'égalité entre femmes et hommes (LEg), la Confédération met à la disposition des employeurs un outil d'analyse standard gratuit pour effectuer des analyses de l'égalité salariale. Les employeurs qui effectuent des analyses de l'égalité salariale conformément à l'art. 13a LEg au moyen de cet outil d'analyse standard peuvent apporter avec la présente déclaration de conformité la preuve d'une méthode scientifique et conforme au droit au sens de l'art. 13c, al. 1 LEg (cf. art. 7, al. 3 de l'ordonnance sur la vérification de l'analyse de l'égalité des salaires). L'outil d'analyse standard (Logib) a été développé au début des années 2000 par le Bureau fédéral de l'égalité entre femmes et hommes (BFEG), avec le soutien d'institutions privées spécialisées. Depuis 2020, Le BFEG propose Logib en tant qu'application Web, gérée par l'Office fédéral de l'informatique et de la télécommunication (OFIT).

1.1 Preuve concernant la sécurité

Une analyse des besoins de protection ainsi que la protection informatique de base ont été élaborées selon les prescriptions de sécurité (protection informatique de base) et mises en vigueur. Les dispositions à prendre pour garantir la sécurité sont exposées de façon transparente et exhaustive en annexe au présent document.

Par la présente, le Bureau fédéral de l'égalité entre femmes et hommes (BFEG) confirme que l'outil d'analyse standard (Logib) est conforme à toutes les prescriptions de la Confédération en matière de sécurité selon l'analyse des besoins de protection et la protection informatique de base. L'application Web ne traite pas de données sensibles. L'application Web fait régulièrement l'objet d'une maintenance et d'un examen des failles de sécurité.

Berne, octobre 2020

Sylvie Durrer

Directrice BFEG

Markus Grossenbacher

Chef de la sécurité
OFIT

Patric Aeberhard

Expert en égalité
salariale BFEG

Annexe à la déclaration de sécurité

Statut En cours d'élaboration, en cours de vérification, approuvé

Version 2020.2

Table des matières

1	Contexte.....	1
1.1	Preuve concernant la sécurité.....	1
2	Introduction à la déclaration de sécurité	4
2.1	Qu'est-ce que Logib ?	4
2.2	Révision de la loi sur l'égalité entre femmes et hommes, art. 13a ss LEg.....	4
2.3	Preuve concernant la sécurité.....	4
2.4	Brève description de la déclaration de sécurité.....	4
3.1	Vue d'ensemble de Logib	5
3.2	Sur quelles bases techniques repose Logib ?.....	5
3.2.1	Interface utilisateur (UI)	5
3.2.2	Back-end.....	5
3.2.3	Analyse R	6
3.3	Où se trouvent les serveurs ?.....	6
3.4	Comment accède-t-on à Logib ?.....	6
3.4.1	Accès interne	6
3.4.2	Accès externe	6
3.5	Vue réseau.....	7
4	Confidentialité.....	8
4.1	Données	8
4.1.1	Qu'advient-il des données pendant l'exécution de l'analyse ?.....	8
4.1.2	Flux de données.....	8
4.1.3	Les données sont-elles enregistrées ?.....	10
4.1.4	Les données sont-elles retraitées ?.....	10
4.1.5	Comment la sécurité des données est-elle garantie ?.....	10
4.1.6	Les données peuvent-elles être consultées ?.....	10
4.2	Transmission des données	11
4.2.1	Cryptage	11
4.3	Suppression des données	11
4.3.1	Comment les données sont-elles supprimées ?	11
4.4	Données personnelles.....	11
4.4.1	Des données personnelles sont-elles lues dans l'application Web ?	11
4.4.2	Qu'advient-il des données personnelles ?	12
4.5	Informations classifiées	12
4.5.1	Des informations classifiées au sens de l'OPrl sont-elles traitées ?	12
4.5.2	Des informations devant faire l'objet d'une protection particulière (données sensibles) en vertu d'une législation spéciale sont-elles traitées dans l'application Web ?	12
5	Disponibilité de l'application	12
5.1	Durée de défaillance.....	12
5.1.1	Quelle est la durée de défaillance maximale admissible ?	12
5.2	Horaires de service.....	12
5.2.1	Quels sont les horaires de service ?	12

5.3	IT Service Continuity Management (ITSCM)	12
5.3.1	La gestion de la continuité des services informatiques (ITSCM) est-elle importante en tant que partie de la gestion de la continuité des affaires (BCM) pour les processus critiques ?.....	12
6	Intégrité.....	13
6.1	L'authenticité, l'exactitude et/ou l'intégrité des données doivent-elles pouvoir être prouvées ?	13
7	Traçabilité.....	13
7.1	Certains processus de travail doivent-ils pouvoir être retracés ?.....	13
8	Pertinence GRAES.....	13
8.1	Logib risque-t-il d'être compromis par des services de renseignement ?.....	13
9	Fichiers journaux.....	13
9.1	Qu'est-ce qu'un fichier journal ?.....	13
9.2	Dans quel but les fichiers journaux sont-ils utilisés ?	14
9.3	Où les fichiers journaux sont-ils enregistrés ?.....	14
9.4	Comment les fichiers journaux sont-ils supprimés ?	14
9.5	Comment la sécurité des données des fichiers journaux est-elle garantie ?....	14
10	Erreurs d'analyse.....	14
11	Annexe.....	15
11.1	Représentation graphique du flux de données Logib	15
12	Glossaire.....	16
13	Références.....	18

Table des illustrations

Illustration 1 : vue d'ensemble de Logib.....	5
Illustration 2 : vue réseau.....	7
Illustration 3 : flux de données Logib	8
Illustration 4 : flux de données Logib [agrandi].....	15

Table des tableaux

Tableau 1 : explication du flux de données Logib	10
Tableau 2 : Glossaire	17

2 Introduction à la déclaration de sécurité

Le présent document donne une vue d'ensemble des mesures de sécurité appliquées à l'outil d'analyse standard (Logib). A partir du chapitre 3.1, ces mesures sont décrites sous forme de questions et réponses.

2.1 Qu'est-ce que Logib ?

Logib [1] est l'outil d'analyse standard de la Confédération pour l'analyse de l'égalité salariale.

En collaboration avec l'Office fédéral de l'informatique et de la télécommunication (OFIT), le Bureau fédéral de l'égalité entre femmes et hommes (BFEG) a développé Logib afin de permettre, d'une part, l'autocontrôle par les employeurs du respect de l'égalité salariale entre les femmes et les hommes, et d'autre part, les contrôles dans le domaine des marchés publics (art. 8, al. 1, let. c LMP).

2.2 Révision de la loi sur l'égalité entre femmes et hommes, art. 13a ss LEg

Depuis l'entrée en vigueur, le 1^{er} juillet 2020, de la loi révisée sur l'égalité entre femmes et hommes (LEg), les entreprises de cent collaborateur-trice-s et plus sont tenues d'effectuer une analyse de l'égalité salariale tous les quatre ans et de la faire contrôler par un organe indépendant. De plus, les travailleur-euse-s et les actionnaires doivent être informés du résultat de l'analyse de l'égalité salariale. Une ordonnance est également entrée en vigueur pour réguler la formation des entreprises chargées de la révision, la vérification des analyses de l'égalité des salaires ainsi que le calendrier [2]. Par conséquent, à compter du 1^{er} juillet, la Confédération est tenue de mettre gratuitement à la disposition des employeurs un outil d'analyse standard selon l'art. 13c, al. 2 LEg.

2.3 Preuve concernant la sécurité

Une analyse des besoins de protection [3] ainsi que la protection informatique de base [4] ont été élaborées selon les prescriptions de sécurité (protection informatique de base) et mises en vigueur.

2.4 Brève description de la déclaration de sécurité

Les principaux points de la présente déclaration de sécurité sont énumérés ci-dessous :

- Les données sont disponibles pour l'utilisateur-trice uniquement pour la durée de la session de navigation en cours et ne sont donc sauvegardées nulle part de façon permanente.
- Les données peuvent uniquement être traitées localement, dans la mémoire cache du navigateur de l'utilisateur-trice. Aucun tiers n'y a accès.
- Dès que le navigateur est fermé, toutes les données sont effacées.
- Les données sont transférées selon le protocole https, c'est-à-dire qu'elles sont cryptées.
- Le serveur de Logib est géré par l'Office fédéral de l'informatique et de la télécommunication.
- L'application Logib se fonde sur des méthodes scientifiques et conformes au droit [5].

3 Architecture

Ce chapitre décrit l'architecture et sa mise en œuvre technique.

3.1 Vue d'ensemble de Logib

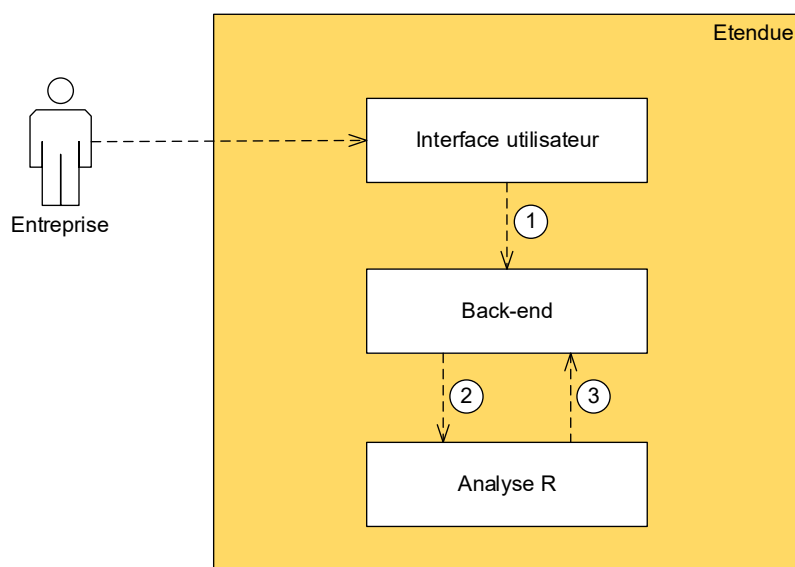


Illustration 1 : vue d'ensemble de Logib

3.2 Sur quelles bases techniques repose Logib ?

3.2.1 Interface utilisateur (UI)

Cette composante sert à l'interaction avec l'utilisateur-trice.

Dans le système présenté ici (étape 2), l'utilisateur-trice n'a pas besoin de s'enregistrer.

- Contrôle de la plausibilité des données transmises (à l'exception de la validation du numéro courant)
- Contrôle syntaxique des données transmises
→ <https://confluence.bit.admin.ch/pages/viewpage.action?pageId=268097910>
- Conversion graphique des données en provenance de la composante d'analyse (R) avec la bibliothèque Highcharts basée sur Javascript

Produit / technologie

Le framework front-end est Oblique / Angular.

Les deux modules Interface utilisateur et Back-end sont réalisés ensemble dans un micro-service.

3.2.2 Back-end

Principales fonctions exécutées dans le module Back-end :

- Lecture des fichiers de données et conversion en fichier JSON
- Transformation des données âge, sexe, années de service
- Validation du numéro courant (non effectuée dans l'UI pour des raisons liées à la performance)
- Envoi des données au module R au format JSON, puis réception des données renvoyées par R également au format JSON

Produit / technologie

.NET Core 3.x

→ Plate-forme logicielle libre et ouverte de la plate-forme .NET, servant au développement et à l'exécution de programmes applicatifs et développée sous la coordination de Microsoft.

Les deux modules Interface utilisateur et Back-end sont réalisés ensemble dans un micro-service et sont regroupés dans un même conteneur.

3.2.3 Analyse R

La composante d'arrière-plan Analyse R se charge uniquement des calculs (base pour : standardisation des salaires, analyse de régression, chiffres du Cockpit). Elle ne génère pas de graphiques, tableaux, etc.

Les données lui sont transmises par le Back-end sous forme de fichier JSON.

Les résultats des calculs sont également renvoyés au Back-end sous forme de fichier JSON.

Les détails sur les attributs sont disponibles dans la description détaillée des interfaces, au chapitre 4.1.2 Flux de données.

Produit / technologie :

- Plumber (REST API) pour la communication entre les modules Back-end et Analyse R.
- Le module Analyse R est implémenté dans son propre conteneur.

3.3 Où se trouvent les serveurs ?

Les serveurs sont situés dans les locaux protégés du centre de calcul de l'Office fédéral de l'informatique et de la télécommunication en Suisse.

3.4 Comment accède-t-on à Logib ?

3.4.1 Accès interne

Les administrateur-trice-s système ainsi que les développeur-euse-s et les testeur-euse-s de l'application disposent nécessairement d'un accès à l'application au moyen d'un rôle utilisateur personnalisé.

3.4.2 Accès externe

Les utilisateur-trice-s des entreprises qui effectuent l'analyse des salaires peuvent utiliser l'application.

3.5 Vue réseau

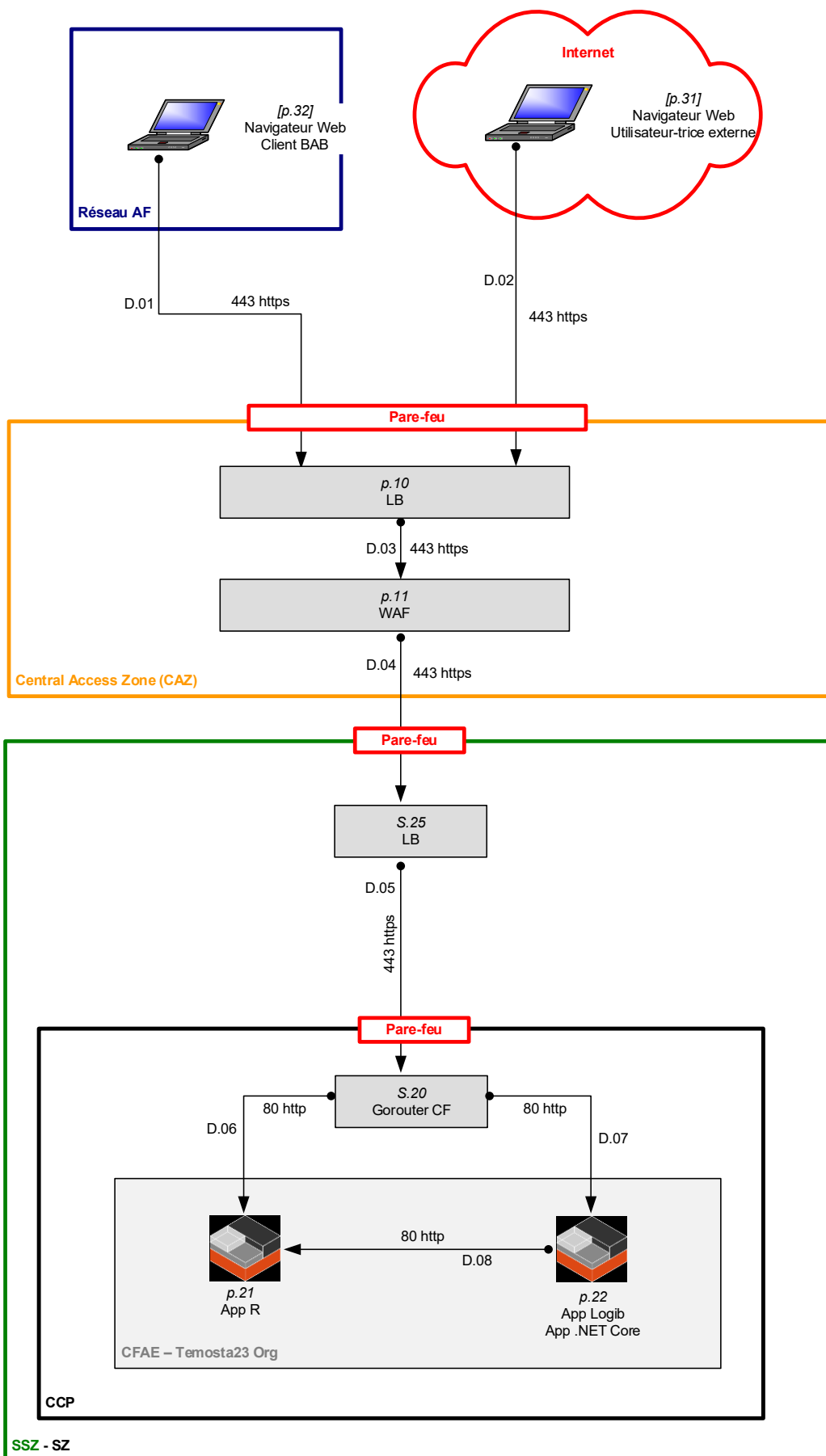


Illustration 2 : vue réseau

4 Confidentialité

4.1 Données

4.1.1 Qu'advient-il des données pendant l'exécution de l'analyse ?

1. Les données sont lues localement dans le navigateur de l'utilisateur-trice.
2. Pour télécharger le navigateur, l'analyse est effectuée sur le serveur de l'Office fédéral de l'informatique et de la télécommunication. Seules les informations absolument nécessaires à cette fin sont transférées, par une connexion cryptée. Aucune donnée n'est sauvegardée sur le serveur au cours de cette procédure, et aucune déduction concernant l'identité de l'entreprise n'est possible. Cette procédure permet par ailleurs de traiter même les fichiers de gros volume contenant les données de grandes entreprises.
3. L'analyse est effectuée dans un outil statistique « R », et non localement dans le navigateur. Le code d'analyse utilisé est assez spécifique : « R » est mieux adapté à sa mise en œuvre que les langages Javascript utilisés dans le navigateur.
4. Le résultat de l'analyse de l'égalité des salaires est renvoyé vers le navigateur.

Le flux de données est représenté comme suit – un schéma plus lisible est disponible en annexe, chapitre 11 :

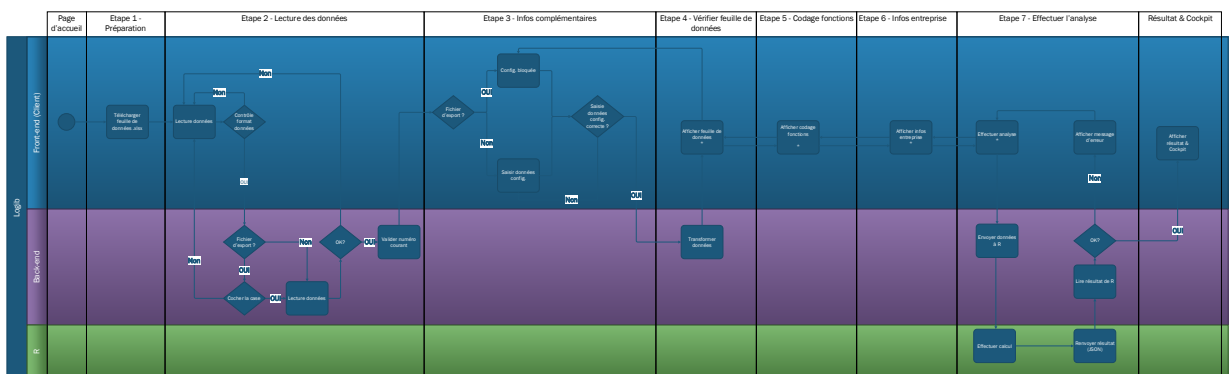


Illustration 3 : flux de données Logib

4.1.2 Flux de données

Explication concernant le flux de données :

Etape 1 – Préparation et procédure	01 – Télécharger feuille de données .xlsx	L'utilisateur-trice peut télécharger la feuille de données sous forme de fichier Excel.
Etape 2 – Lecture des données	02 – Lecture données	La feuille de données remplie par l'entreprise est lue dans Logib.
	03 – Contrôle format données	Le format de la feuille de données est vérifié.
	04 – Fichier d'export ?	La feuille de données est-elle un fichier d'export ? OUI / NON

	05 – Cocher la case	S'il s'agit d'un fichier d'export, la case est cochée.
	06 – Lecture données	Les données sont lues dans le Back-end.
	07 – Lecture réussie ?	La procédure « Lecture des données » a-t-elle fonctionné ? OUI / NON
	08 – Valider numéro courant	Le numéro courant est validé [→ les données sont envoyées au Back-end, qui recherche d'éventuels doublons].
Etape 3 – Informations complémentaires	09 – Fichier d'export ?	La feuille de données est-elle un fichier d'export ? OUI / NON
	10 – Config. bloquée	Il est impossible de saisir des données de configuration à l'étape 3.
	11 – Saisir données config.	Les données de configuration doivent être saisies.
	12 – Saisie données config. correcte ?	Les données de configuration ont-elles été correctement saisies ? OUI / NON
Etape 4 – Vérifier la feuille de données	13 – Transformer données	Les données de la feuille de données sont transformées.
	14 – Afficher feuille de données	La feuille de données est affichée.
Etape 5 – Confirmer le codage des fonctions	15 – Afficher codage fonctions	Le codage des fonctions s'affiche (les fonctions sont reprises de l'étape « Vérifier la feuille de données »).
Etape 6 – Informations sur l'entreprise	16 – Afficher infos entreprise	Des informations sur l'entreprise peuvent être saisies (facultatif).
Etape 7 – Effectuer l'analyse	17 – Effectuer analyse	L'analyse est effectuée.
	18 – Envoyer données à R	Seules les données nécessaires sont envoyées à R.
	19 – Effectuer calcul	Le calcul est effectué dans R.
	20 – Renvoyer résultat (JSON)	Le résultat est renvoyé au serveur.
	21 – Lire résultat de R	Le résultat est lu par le serveur.
	22 – OK ?	Résultat OK ? OUI / NON

	23 – Afficher message d'erreur	Si le résultat n'est pas OK, un message d'erreur s'affiche.
Résultat & Cockpit	24 – Afficher résultat & Cockpit ¹	Si le résultat est OK, le résultat de l'analyse et le Cockpit s'affichent pour l'utilisateur-trice.

Tableau 1 : explication du flux de données Logib

Remarque : toutes les étapes marquées d'un « * » (soit n° 14, 15, 16, 17) peuvent être consultées en mode « Lecture seule » une fois l'analyse effectuée.

4.1.3 Les données sont-elles enregistrées ?

Aucune donnée n'est enregistrée de façon permanente. Voir également point 4.3.

4.1.4 Les données sont-elles retraitées ?

Les données ne seront pas retraitées par des tiers.

4.1.5 Comment la sécurité des données est-elle garantie ?

La sécurité des données repose sur trois piliers :

1. Connexion sécurisée

Les données sont transmises par une connexion cryptée TLS.

TLS (Transport Layer Security) est un protocole cryptographique garantissant la sécurité des transmissions de données sur Internet.

2. Données anonymes (aucun nom, prénom ou nom de fonction n'est transmis.)

Les données transmises sont anonymisées : leur contenu n'est donc pas sensible.

Pour cela, les données lues par l'utilisateur-trice doivent avoir été correctement préparées. Si des noms et prénoms se sont glissés par erreur dans le jeu de données, des données personnalisées sont alors traitées. C'est pourquoi il importe de veiller à l'anonymisation selon les instructions.

L'application Logib ne peut pas influencer le contenu des données livrées par l'utilisateur-trice.

3. Pas d'enregistrement des données

Les données ne sont pas enregistrées et ne sont disponibles que pendant la session en cours.

4.1.6 Les données peuvent-elles être consultées ?

Les données ne peuvent être consultées que par l'utilisateur-trice. Les documents générés ne sont sauvegardés nulle part et ne sont pas transmis à des tiers. Ils peuvent être téléchargés par l'utilisateur-trice pendant la session en cours.

¹ Les modèles sont envoyés par le Front-end au Back-end, où ils sont remplis avec les données correspondantes → openxml remplit les variables des modèles.

4.2 Transmission des données

4.2.1 Cryptage

Les données sont cryptées selon le protocole TLS (https).

4.3 Suppression des données

4.3.1 Comment les données sont-elles supprimées ?

Dès que le navigateur Web est fermé, les données qui ont été lues sont également supprimées. L'utilisateur-trice n'a donc pas la possibilité de fermer momentanément son navigateur et d'accéder ultérieurement aux données lues auparavant et/ou à leur analyse. Avec la fonction « Exporter feuille de données au format Excel », l'utilisateur-trice a la possibilité à tout moment d'enregistrer localement les données enregistrées dans la mémoire cache du navigateur pour les lire à nouveau ultérieurement dans Logib et poursuivre l'analyse.

4.4 Données personnelles

4.4.1 Des données personnelles sont-elles lues dans l'application Web ?

Un fichier contenant tou-te-s les collaborateur-trice-s, en l'occurrence la feuille de données au format Excel, est lu dans la mémoire cache locale du navigateur. Les données obligatoires pour l'analyse sont les suivantes : mois de référence, année de référence, numéro courant, âge, sexe, années de service, formation, fonction, niveau de compétence au sein de l'entreprise, position professionnelle, degré d'activité ou heures payées, ainsi que les différents éléments du salaire. D'autres données peuvent être saisies, telles que le nom, le numéro AVS et l'adresse des différentes personnes. Toutefois, cela n'est pas recommandé si l'on souhaite préserver la confidentialité.

Seules les données nécessaires à l'analyse sont transmises au serveur R (cf. point 4.1.1) :

- Le numéro courant est anonymisé.
- La fonction n'est pas utilisée pour l'analyse et est uniquement enregistrée localement dans la mémoire cache du navigateur.

Pendant l'analyse, les données personnelles sont visibles dans le navigateur ouvert, mais dès que ce dernier est fermé, les données lues sont effacées.

Dans l'étape de l'assistant « Informations sur l'entreprise », des données concernant l'entreprise peuvent être saisies facultativement, p. ex. la raison sociale, l'adresse, la personne de contact, le numéro de téléphone et l'adresse e-mail. Si elles sont utilisées, ces informations sont également transmises au Back-end et intégrées dans les documents de résultat ainsi que dans le fichier d'export (p. ex. Excel)².

² Les modèles sont envoyés par le Front-end au Back-end, où ils sont remplis avec les données correspondantes → openxml remplit les variables des modèles.

4.4.2 Qu'advient-il des données personnelles ?

Elles sont envoyées au Back-end pour le calcul de l'égalité salariale et y sont stockées dans la mémoire uniquement pour la durée nécessaire à l'analyse en cours. Actuellement, les données ne sont pas persistantes. Voir l'explication détaillée au point 4.1.1.

4.5 Informations classifiées

4.5.1 Des informations classifiées au sens de l'OPRI sont-elles traitées ?

Selon l'analyse des besoins de protection TEMOSTA23 V.1.1, aucune donnée / information classifiée selon l'OPRI n'est enregistrée, traitée ou analysée par le système.

4.5.2 Des informations devant faire l'objet d'une protection particulière (données sensibles) en vertu d'une législation spéciale sont-elles traitées dans l'application Web ?

Selon l'analyse des besoins de protection TEMOSTA23 V.1.1, aucune donnée sensible n'est enregistrée, traitée ou analysée par le système.

5 Disponibilité de l'application

5.1 Durée de défaillance

5.1.1 Quelle est la durée de défaillance maximale admissible ?

La durée de défaillance maximale admissible est de 12 heures, ce qui correspond à la classe de disponibilité 1 selon le catalogue des services.

5.2 Horaires de service

5.2.1 Quels sont les horaires de service ?

Le service est disponible du lundi au vendredi, de 7h00 à 18h00.

5.3 IT Service Continuity Management (ITSCM)

5.3.1 La gestion de la continuité des services informatiques (ITSCM) est-elle importante en tant que partie de la gestion de la continuité des affaires (BCM) pour les processus critiques ?

L'ITSCM n'est pas importante dans le cadre du BCM. En cas d'urgence, l'ensemble du site Web peut être temporairement indisponible. Dans ce cas, des mesures organisationnelles sont élaborées, comme la fourniture à court terme de Logib avec une technologie différente. Tout en maintenant les mêmes standards de sécurité.

6 Intégrité

6.1 L'authenticité, l'exactitude et/ou l'intégrité des données doivent-elles pouvoir être prouvées ?

Selon l'analyse des besoins de protection, aucune exigence spéciale n'est imposée en matière d'intégrité.

Comme l'application fonctionne en ligne et que le résultat de l'analyse n'est renvoyé qu'à la personne qui a transmis les données, il n'y a pas lieu d'implémenter une fonctionnalité pour repérer une quelconque manipulation des données.

7 Traçabilité

7.1 Certains processus de travail doivent-ils pouvoir être retracés ?

Selon l'analyse des besoins de protection de la Confédération, aucune exigence spéciale n'est imposée en matière de traçabilité.

Le chapitre 9 décrit les données qui sont enregistrées dans le fichier journal et l'endroit où elles sont sauvegardées.

8 Pertinence GRAES

8.1 Logib risque-t-il d'être compromis par des services de renseignement ?

L'examen effectué dans le cadre de l'analyse des besoins de protection a révélé que Logib ne relevait pas du processus GRAES et n'était pas exposé à un risque de manipulation à des fins de renseignement.

9 Fichiers journaux

9.1 Qu'est-ce qu'un fichier journal ?

Lors de l'utilisation de l'application, des fichiers journaux (fichiers log) standard sont créés pour permettre l'accomplissement de certaines tâches relevant de l'exploitation informatique. L'exploitation informatique, bien que gérée par le BFEG sur le plan organisationnel, est assurée par l'OFIT sur le plan technique, en un autre lieu. Ainsi, les fichiers journaux sont créés dans des locaux de l'OFIT et donc soumis aux conventions de sécurité de l'OFIT.

L'application Logib ne crée pas de fichier journal à proprement parler. En revanche, les conteneurs Cloud Foundryregistrent des fichiers journaux sur la console correspondante. Ces fichiers journaux persistent un certain temps et peuvent être interrogés par l'équipe de développeurs.

9.2 Dans quel but les fichiers journaux sont-ils utilisés ?

La plate-forme Cloud Foundry, en tant que base technique, comprend diverses fonctions destinées à protéger les infrastructures fédérales contre les cyberattaques. C'est pourquoi les adresses IP des utilisateur-trice-s, notamment, sont enregistrées dans des fichiers journaux. Pour des raisons liées à la sécurité, ces informations ne sont pas communiquées par l'OFIT à d'autres équipes. De la même façon, ces informations ne parviennent pas à Logib / à l'équipe qui garantit l'exploitation de Logib et continue à développer l'application.

Les fichiers journaux pour l'application Logib sont utilisées pour l'analyse des éventuelles erreurs signalées par les utilisateur-trice-s. Ils contiennent uniquement des détails techniques concernant les erreurs, qui y sont consignés avec un identifiant de requête. Cela permet de repérer où différentes erreurs se sont produites au cours d'un processus. Les informations qu'ils contiennent ne permettent pas de remonter jusqu'à l'utilisateur-trice. A chaque session du Front-end Logib, les données suivantes sont enregistrées temporairement dans des fichiers journaux : date, heure, déclenchement de la 1^{re} analyse dans l'assistant et informations sur les erreurs / alertes. Aucune donnée concernant les utilisateur-trice-s n'est enregistrée dans les fichiers journaux.

De plus, séparément du Front-end, la plate-forme Cloud Foundry identifie l'adresse IP, comme décrit plus haut.

9.3 Où les fichiers journaux sont-ils enregistrés ?

Les fichiers journaux sont enregistrés sur la plate-forme Cloud Foundry. Cette plate-forme est gérée par l'équipe CCP de l'OFIT. L'équipe CCP dépend d'un secteur distinct sur le plan organisationnel.

9.4 Comment les fichiers journaux sont-ils supprimés ?

Les fichiers journaux enregistrés sur la plate-forme Cloud Foundry sont conservés pendant 90 jours pour des raisons de sécurité. Ils sont ensuite automatiquement supprimés par la plate-forme elle-même.

Leur suppression peut être configurée sur la plate-forme.

9.5 Comment la sécurité des données des fichiers journaux est-elle garantie ?

La plate-forme Cloud Foundry est mise à disposition et exploitée par l'OFIT. C'est donc l'équipe CCP de l'OFIT qui assume la responsabilité de la sécurité des fichiers journaux. Les accès sont réglementés par le concept de sécurité [SIPD] et de règlement des accès pour l'équipe CCP.

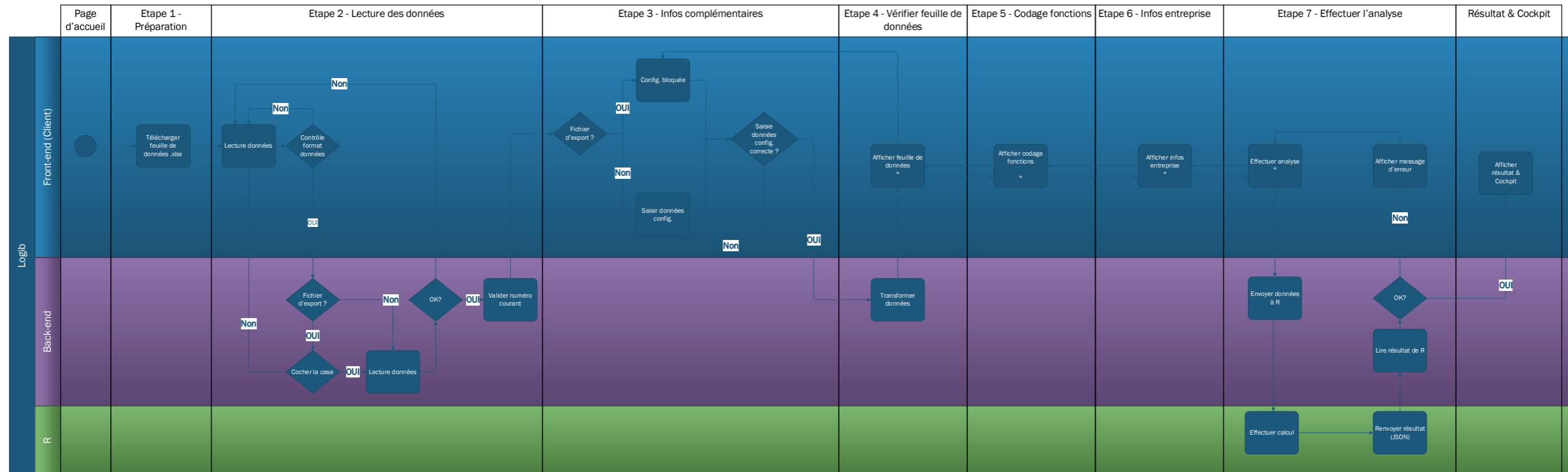
10 Erreurs d'analyse

Si une erreur survient au cours de l'utilisation de Logib, l'utilisateur-trice reçoit un message d'erreur sous forme d'une notification Oblique, et les détails techniques de l'erreur sont consignés dans un fichier journal, comme décrit au chapitre 9.

11 Annexe

11.1 Représentation graphique du flux de données Logib

Voici une représentation graphique du flux de données Logib :



Remarque :

* Une fois que l'analyse a été effectuée, l'utilisateur peut consulter les étapes marquées d'un « * » en mode « Lecture seule ».



12 Glossaire

Terme / abréviation	Signification
.NET Core 3.x	Plate-forme logicielle libre et ouverte de la plate-forme .NET, servant au développement et à l'exécution de programmes applicatifs et développée sous la coordination de Microsoft
BCM	Business Continuity Management, gestion de la continuité des affaires
Marchés publics	Selon l'art. 8, al. 1, let. c LMP [6]
OFIT	Office fédéral de l'informatique et de la télécommunication [7]
Réseau AF	Réseau de l'administration fédérale
CAZ	Central Access Zone, zone d'accès centrale
Cloud Foundry, CF	Plate-forme cloud Kubernetes stratégique de l'OFIT
Conteneur	Les conteneurs constituent une tendance récente dans l'informatique. Ils regroupent une application et tous les fichiers nécessaires à son exécution dans un paquet simple à utiliser.
BFEG	Bureau fédéral de l'égalité entre femmes et hommes [8]
LEg	Loi sur l'égalité entre femmes et hommes
HTTPS	Hypertext Transfer Protocol Secure, protocole de communication Web comportant un cryptage du transport, c.-à-d. que les données sont protégées contre les interceptions lors de leur transmission.
OPri	Ordonnance concernant la protection des informations de la Confédération [9]
ITSCM	IT Service Continuity Management, gestion de la continuité des services informatiques
JavaScript	Langage de programmation initialement développé pour le protocole HTML dynamique dans les navigateurs Web
JSON	JavaScript Object Notation, format de données compact, dans une forme textuelle

Terme / abréviation	Signification
	simple à lire, utilisé pour l'échange de données entre deux applications
LB	Load Balancer, répartiteur de charges dans une infrastructure informatique
Fichier journal, fichier log	Un fichier journal est un enregistrement automatique en continu de toutes les actions ou d'une action en particulier réalisées dans le cadre d'un processus dans un système informatique.
Logib	Outil d'analyse standard de la Confédération pour l'analyse de l'égalité des salaires
Matomo	Programme d'analyse gratuit
Oblique / Angular	Framework Front-end pour les marques suisses d'UI
Plumber (REST API)	Programme permettant de créer une interface d'application (Application Programming Interface, API) garantissant la communication entre le module Back-end et le module R
R	Programme (ou langage de programmation) open source pour les calculs statistiques et les graphiques
GRAES	Gestion des risques des activités d'espionnage de services de renseignements, méthode de gestion des risques développée par l'UPIC
ABP	Analyse des besoins de protection [3]
SSZ	Shared Service Zone
SZ	Server Zone
TLS	Transport Layer Security, également connu sous le nom de Secure Sockets Layer (SSL), protocole de cryptage hybride pour la sécurité des transmissions de données sur Internet
UI	User Interface, interface utilisateur, décrivant la façon dont l'utilisateur-interagit avec la machine
WAF	Web Application Firewall, procédure destinée à protéger les applications Web contre les attaques utilisant le protocole http

Tableau 2 : Glossaire

13 Références

- [1] Bureau fédéral de l'égalité entre femmes et hommes (BFEG), « Analyser l'égalité salariale – en toute simplicité et sécurité avec Logib », [en ligne]. Disponible sur : <https://www.ebg.admin.ch/ebg/fr/home/prestations/logib.html>. [Accès le 26.06.2020].
- [2] Bureau fédéral de l'égalité entre femmes et hommes (BFEG), « Questions et réponses concernant l'analyse de l'égalité salariale selon la LEg », [en ligne]. Disponible sur : <https://www.ebg.admin.ch/ebg/fr/home/themes/travail/egalite-salariale/analyse-LEg.html>. [Accès le 26.06.2020].
- [3] Unité de pilotage informatique de la Confédération (UPIC), « P041 – Analyse des besoins de protection (Schuban) », 28.01.2020. [En ligne]. Disponible sur : https://www.isb.admin.ch/isb/fr/home/ikt-vorgaben/prozesse-methoden/p041-schutzbedarfsanalyse_schuban.html. [Accès le 26.06.2020].
- [4] Unité de pilotage informatique de la Confédération (UPIC), « Si001 – Protection informatique de base dans l'administration fédérale », 22.12.2019. [En ligne]. Disponible sur : https://www.isb.admin.ch/isb/fr/home/ikt-vorgaben/sicherheit/si001-ikt-grundschutz_in_der_bundesverwaltung.html. [Accès le 26.06.2020].
- [5] Bureau fédéral de l'égalité entre femmes et hommes (BFEG), « Déclaration de conformité – Outil d'analyse standard (Logib) », 18.03.2020. [En ligne]. Disponible sur : [https://www.ebg.admin.ch/dam/ebg/fr/dokumente/lohngleichheit/logib/konformitaetserklaerung_logib.pdf.download.pdf/D%C3%A9claration%20de%20conformit%C3%A9_Outil%20d%E2%80%99analyse%20standard%20\(Logib\)_V2020.1.pdf](https://www.ebg.admin.ch/dam/ebg/fr/dokumente/lohngleichheit/logib/konformitaetserklaerung_logib.pdf.download.pdf/D%C3%A9claration%20de%20conformit%C3%A9_Outil%20d%E2%80%99analyse%20standard%20(Logib)_V2020.1.pdf). [Accès le 26.06.2020].
- [6] Le Conseil fédéral, « 172.056.1 – Loi fédérale sur les marchés publics (LMP) », 20.06. 2020. [En ligne]. Disponible sur : <https://www.admin.ch/opc/fr/classified-compilation/19940432/index.html>. [Accès le 26.06.2020].
- [7] Office fédéral de l'informatique et de la télécommunication (OFIT), « Page d'accueil », [en ligne]. Disponible sur : <https://www.bit.admin.ch/bit/fr/home.html>. [Accès le 26.06.2020].
- [8] Bureau fédéral de l'égalité entre femmes et hommes (BFEG), « Page d'accueil », [en ligne]. Disponible sur : <https://www.ebg.admin.ch/ebg/fr/home.html>. [Accès le 26.06.2020].
- [9] Le Conseil fédéral, « Ordonnance concernant la protection des informations de la Confédération (OPrI) », 01.01.2018. [En ligne]. Disponible sur : <https://www.admin.ch/opc/fr/classified-compilation/20070574/index.html>. [Accès le 03.07.2020].