PLATEFORME des DPD des CPAS
(Fédération des CPAS)

GESTION DES LOGS DE SÉCURITÉ

11 OCTOBRE 2022

AGENDA

- Préliminaire: Gestion des Accès (Rappel)
- Journalisation : les obligations et recommandations telles que définies par les lois et règlements divers
- Les différentes catégories de logs
- Responsabilités pour prise et consultation de logs
- Procédure: portée, cibles, moyens
- Approche du DPD pour entreprendre les contrôles qui lui incombent dans son CPAS:
    - Implication de la hiérarchie pour valider la procédure ?
    - Comment informer les employés de ces contrôles ?
    - Échantillonnage ou pas ?
    - Périodicité du contrôle ?
    - Brève présentation des écrans de recherche dans « IRIS »
- Varia – Echanges de Points de vue…

Rappel concernant la gestion des Accès (1 de 2)

L'ancienne appellation "Responsable Accès Entité" a été remplacée par « Gestionnaire d'Accès Principal".

Le GAP peut avoir tous les accès au portail de la sécurité sociale et à toutes les applications du SPP Intégration sociale (Rapport unique, Ebox, etc).

Le GAP est le/la Directeur/trice général(e) ou le/la Secrétaire.

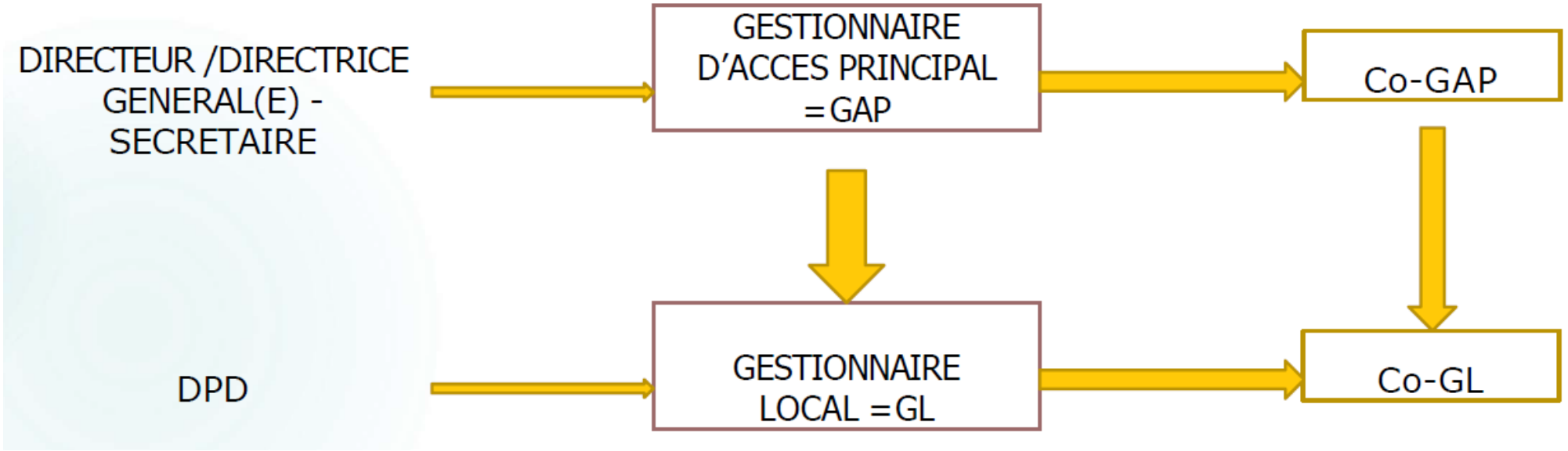
Le GAP a des responsabilités juridiques: traitement des DIMONA et déclarations multifonctionnelles entre autres.

Le GAP a accès à toutes les qualités : Action sociale, Employeur PPL, Gestionnaire de pensions, etc. et peut actionner les nouvelles qualités.

Le GAP est le seul à pouvoir créer le Gestionnaire local (GL), rôle qui incombe d'office au DPD.

Si le DPD n'a pas été annoncé au SPP IS, le GAP ne pourra pas lui donner le rôle de GL.

Rappel concernant la gestion des Accès (1 de 2)



Pour des raisons évidentes de sécurité (absence longue durée, immobilisation, décès), le GAP peut créer un CO-GAP qui aura les mêmes accès et possibilités techniques sauf une: il ne pourra pas créer lui-même un autre CO-GAP.
Le DPD - GL pourra également créer un CO-GL avec l'autorisation du Directeur général – de la Directrice générale – du/de la Secrétaire.

MAIS QUI PEUT CRÉER UN GAP ?

Seul le Président du CPAS pourra aller sur le site

https://www.csam.be/fr/gestion-gestionnaires- acces.html

pour créer le GAP.

Attention, le Président devra être sur la liste des salariés du CPAS (vérification par l'ONSS) et/ou en ordre de BCE (Banque Carrefour des Entreprises) pour avoir accès au site https://www.csam.be/fr/gestion-gestionnaires-acces.html et donner le rôle de GAP au DPD.

Les Obligations (1 de 2)

En pratique, il existe bien peu de règles ou obligations concernant la gestion des logs du point de vue du DPD.
On peut citer:

- **GDPR**: rien de formellement décrit comme « obligation » à cet égard
- **BCSS**: https://www.ksz-bcss.fgov.be/sites/default/files/assets/protection_des_donnees/bld_log_gestion_logs.pdf
- **Autres documentations / informations y relatives:**
  - **UCVW**: pour info, voir https://www.uvcw.be/no_index/articles-pdf/download/2671.pdf
  - **BOSA** (initiative « FISP » (doc NL uniquement, mais bientôt mises à jour disponibles): https://bosa.belgium.be/sites/default/files/documents/Handleiding%20voor%20logging%20en%20monitoring.pdf

Les Obligations (2 de 2)

Selon les Normes Minimales de la BCSS, toute organisation doit mettre en place une procédure formelle de gestion de logs, la valider, la communiquer et la maintenir.

Pour un CPAS, cela consiste notamment en:

1. Disposer d'une procédure, en contrôler le respect et connaître le contenu des fichiers de logging
2. Contrôler l'accès aux données de logging
3. Réaliser des contrôles périodiques afin de s'assurer du respect des mesures qui la concernent
4. Analyser, rapporter (aux responsable de la gestion journalière) et évaluer régulièrement le résultat de la gestion des logs

5. En tant que propriétaire de l'application(*), l'organisation doit prévoir et gérer les fichiers de logging de sécurité de l'information et de protection de la vie privée. Concrètement, cela implique la gestion, la conservation, l'archivage des fichiers de journalisation de sécurité de l'information et de protection de la vie privée et leur suppression à l'issue de leur durée de conservation

(*) càd SPP IS (e.a. via Smals), société de soft (p.ex. Novadis), mais aussi CPAS pour leurs applications internes

Contrôles : Approche du DPD

Les contrôles seront évidemment proportionnels à la taille du CPAS, du nombre de ses clients, des applications utilisées et (surtout) du temps dont dispose le DPD.
En pratique, les dispositions minimales suivantes devraient être observées:

- Implication de la hiérarchie pour valider la procédure et les contrôles:
  Le DPD aura communiqué la procédure, l'aura faite valider et lui en fera rapport (au minimum à l'occasion de son rapport annuel)
- Information des employés de ces contrôles:
  Tous les agents doivent savoir que tous leurs accès sont loggués, qu'un contrôle aléatoire est organisé et, s'il en font l'objet, qu'ils devront justifier la raison de tout accès
- Échantillonnage : il est recommandé de procéder sur base de critères aléatoires
- Périodicité du contrôle : au minimum trimestriellement (bien qu'il n'existe pas de règle absolue)
- Conclusions/conséquences des résultats et constatations suite aux contrôles:
  - Au niveau de l'agent: voir sanctions prévues dans règlement de travail
  - Au niveau DPO: si abus manifeste, évaluer nécessité d'une déclaration de violation de données
  - Au niveau Direction: évaluer besoins de révision + communication/formation

Les différentes catégories de logs

- **Logs techniques / d'infrastructure :** Logs créés pour l'analyse technique et la récupération technique des actifs TIC.
  Temps de rétention souhaitable 6 mois sauf si d'autres dispositions légales prévoient une période de stockage plus longue.
- **Logs d'entreprise :** Logs créés pour analyser et restaurer les systèmes transactionnels commerciaux.
  Temps de rétention souhaitable 2 ans sauf si d'autres dispositions légales prévoient une période de stockage plus longue.
- **Logs de sécurité :** Logs créés dans le but de détecter et / ou d'analyser les événements et les incidents de sécurité.
  Temps de rétention souhaitable 5 ans sauf si d'autres dispositions légales prévoient une période de stockage plus longue.
- **Les « Privacy Logs » :** Logs créés pour répondre aux règles de confidentialité et y répondre.
  Temps de rétention: en règle générale, 10 ans, sauf exceptions prévues au niveau des lois applicables

Responsabilités

Données personnelles (« privacy logs ») : Qui est responsable de leur collecte et qui peut/doit consulter?

Cfr. https://www.ksz-bcss.fgov.be/sites/default/files/assets/protection_des_donnees/bld_log_gestion_logs.pdf

Une organisation doit mettre en place une procédure formelle de gestion de logs, la valider, la communiquer et la maintenir :		SPP-IS		SMALS		BCSS		MAISONS DE SOFT		CPAS	
1	un système de logging opérationnel	●	✓		✓		✓		✓		✓
2	le contrôle du respect de la procédure et du contenu des fichiers de logging	●	✓	●	✓					●	✓
3	la gestion, la conservation, l'archivage des fichiers de logging de sécurité de l'information et de protection de la vie privée et leur suppression à l'issue de leur durée de conservation,	●									
4	la décision d'inclure les données de logging dans le plan de continuité de l'organisation,	●	✓							●	✓
5	l'accès contrôlé aux données de logging					●					✓
6	en tant que propriétaire de l'application, l'organisation doit prévoir et gérer les fichiers de logging de sécurité de l'information et de protection de la vie privée. Par exemple au niveau du moniteur transactionnel, du système d'exploitation, du système de gestion des autorisations, de la gestion et de la mise à jour des banques de données	●	✓	●		●		●			
7	l'organisation doit réaliser des contrôles périodiques afin de s'assurer du respect des mesures qui la concernent		✓		✓		✓		✓		✓
8	tout utilisateur d'une application de la sécurité sociale ou d'une application ayant recours au réseau de la sécurité sociale doit être informé de l'existence de la gestion des logs et des objectifs de la gestion de logs	●	✓								✓

● : Doit collecter; ✓ : Peut, voire doit consulter/contrôler

Procédure

- **Portée:**
  La procédure fera la distinction selon que les recherches relèvent des besoins du DPD ou bien d'une enquête à l'initiative de l'inspection afin de préciser les filtres à appliquer.
- **Cibles:**
  La procédure précisera, par le contexte des recherches entreprises, quels sont les filtres à appliquer afin de mieux cerner les données appartenant aux catégories suivantes:
    - Agents
    - Personnes concernée
    - Inspecteur
- **Moyens:**
  L'outil principal, pour le DPD, sera IRIS (voir présentation ci-après) pour les application publiées sur le portail de la Sécurité Sociale. Tout autre responsable d'un logiciel traitant des données personnelles devra prévoir les moyens de collecte et de consultation de « privacy logs ».
  Selon les besoins, de nombreuses autres sources pourront être consultées (e.g.: logs des proxies, des firewalls, des DNS) et devront donc être documentées en fonction des résultats qu'elles pourraient délivrer (p.ex., recherches forensiques)

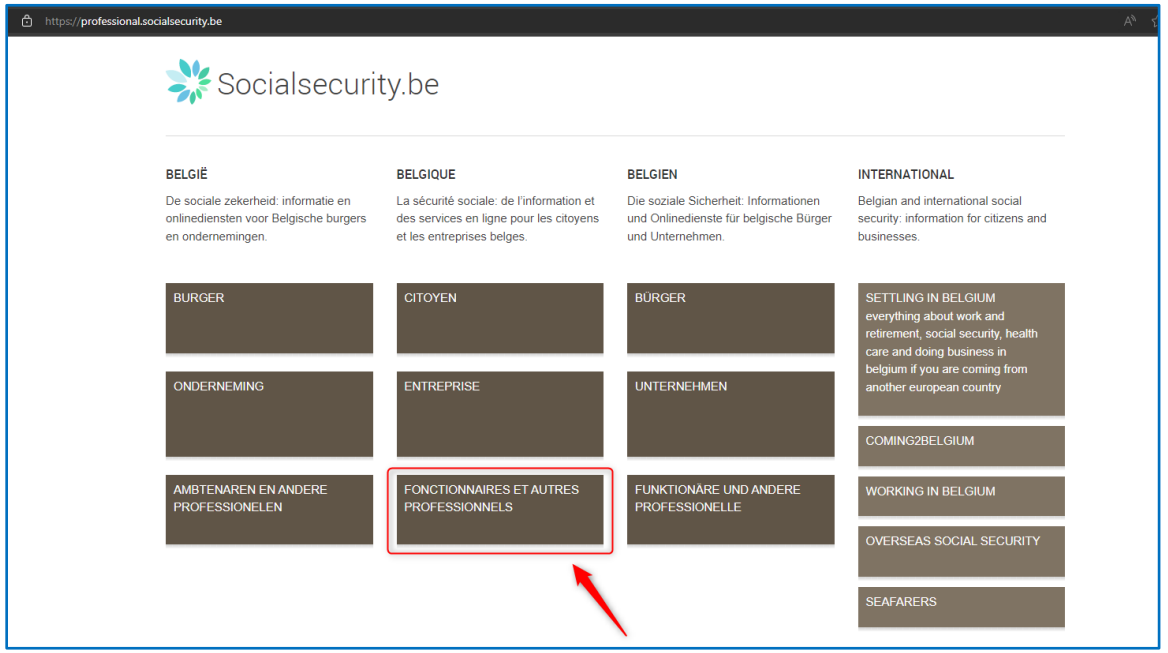
Consultations dans « IRIS » (1 de 4)

Conditions :

- Disposer d´un accès fonctionnaire sur le portail de la Sécurité Social et être autorisé à accéder à l´application (via votre gestionnaire local).
- Disposer d´une carte d´identité électronique et d´un lecteur de carte.

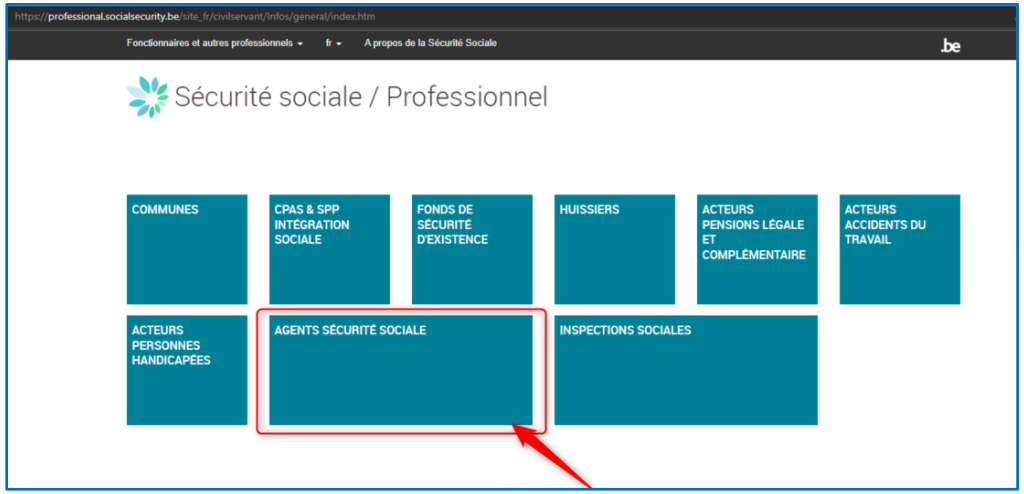
Droits accordés:

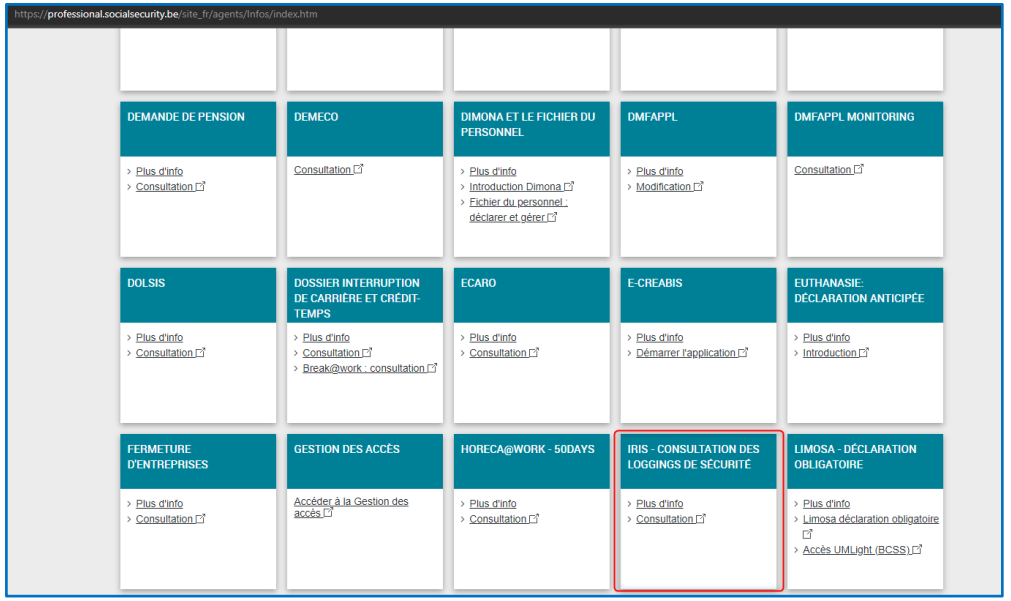
- Responsable sécurité d´une institution : peut accéder aux logging générés par les personnes de son institution
- Responsable sécurité d´un service d´inspection : peut accéder aux logging sécurité générés par les inspecteurs de son institution.

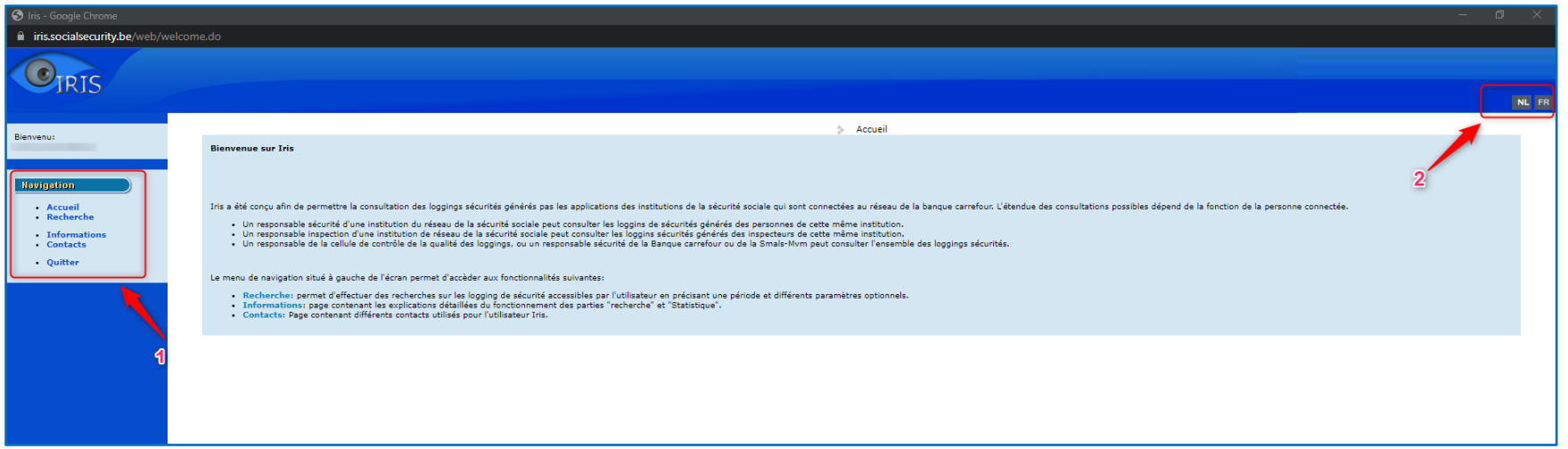


https://iris.prd.ext.socialsecurity.be/app026/iris/welcome.do

Consultations dans « IRIS » (2 de 4)

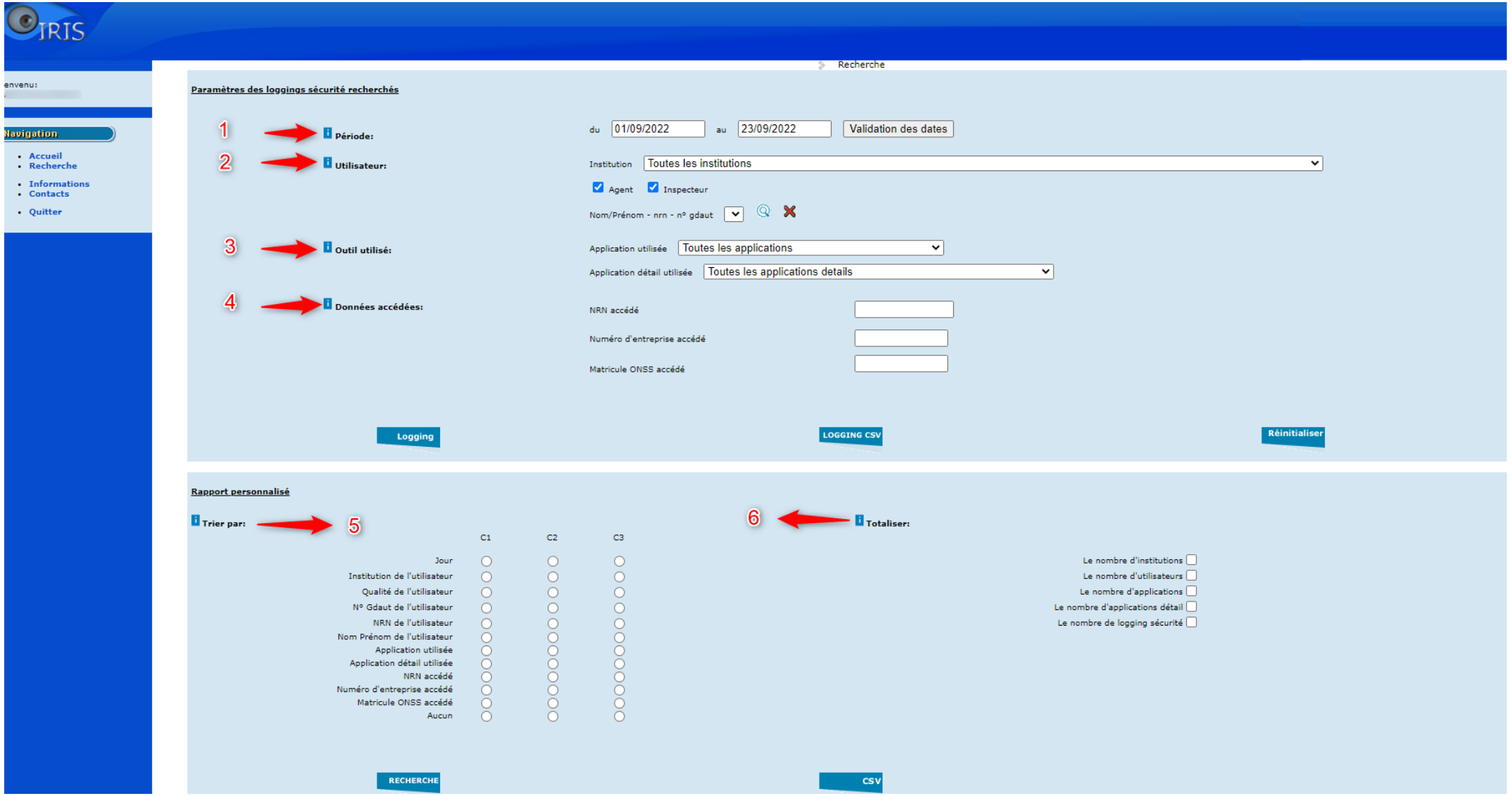






Consultations dans « IRIS » (3 de 4)

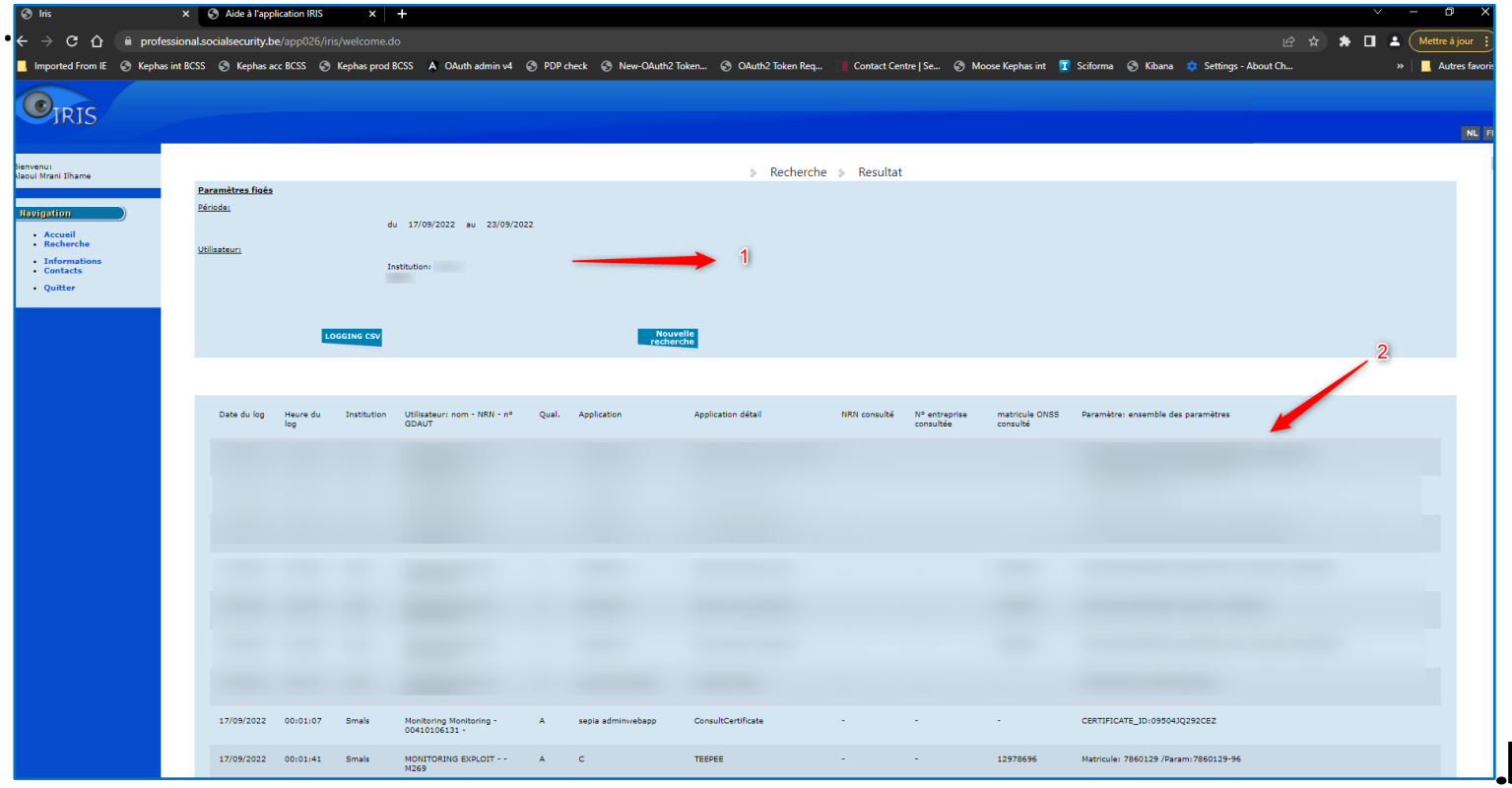
Écran principal: RECHERCHES



Consultations dans « IRIS » (4 de 4)

Résultat(s) de la recherche

Certains résultats du tableau (par exemple, les applications, les institutions) sont des liens hypertexte sur lesquels l´utilisateur peut cliquer afin de préciser la recherche.
Dans ce cas, la page de recherche sera à nouveau affichée, dans laquelle les paramètres figés seront pré-alimentés ainsi que le champ cliqué.



Questions – Échanges de Points de Vue

SPP Intégration sociale, Lutte contre la Pauvreté, Economie sociale et Politique des Grandes Villes

Centre administratif Botanique
Finance Tower
Boulevard du Jardin Botanique 50 boîte 165
1000 Bruxelles

POD MAATSCHAPPELIJKE INTEGRATIE
BETER SAMEN LEVEN
SPP INTÉGRATION SOCIALE
MIEUX VIVRE ENSEMBLE

Contactez-nous

lundi au vendredi de 8h30 à 12h30 et de 13h à 16h30 (vendredi jusque 16h) via

+32 2 508 85 86 ou… +32 508 8430
question@mi-is.be mi.dpo@mi-is.be
www.mi-is.be

Suivez-nous