Bruxelles, le 4 février 2020

Monsieur Arnaud Vajda
Directeur du service d'encadrement P&O
North Galaxy
Bld du Roi Albert II, 33 boite 10
1030 BRUXELLES

SECRETARIAT FEDERAL

Nos réf. : 0203_A_20200204

Vos réf. :

Objet **ICT : Code de déontologie et autres**

Monsieur le Président du CIC personnel,

Suite à la réunion du Comité intermédiaire de Concertation n° 169 en matière de personnel de ce 1er octobre 2019, l'UNSP vous a transmis une liste non exhaustive de ses questions et remarques le 21 octobre 2019 (référence du courrier 0188_A_20191021).

Une nouvelle version du code de déontologie ICT nous est soumise à la concertation ce mardi 11 février.

Dans ce nouveau projet, nous remarquons que quelques-unes de nous remarques ont été prises en considération. Nous en remercions les personnes ayant élaboré ce document.

Néanmoins, certaines questions et remarques, primordiales selon nous, n'ont visiblement pas été considérées.

En l'état actuel, les agents nous ont signalé qu'ils ressentent ce code comme une énième procédure de contrôle et non comme un outil pédagogique et une protection pour les agents. C'est regrettable.

De même, par certains aspects, ce code risque de mettre de véritables bâtons dans les roues des agents, leur empêchant de réaliser leurs missions…

Nous pensons, par exemple, à l'exclusion des clefs USB sans la mise en route d'une alternative utilisable dans toutes les situations.

Aussi, afin que la réunion du 11 février prochain puisse s'organiser dans les meilleures conditions, nous souhaitons que les différents points suivants soient évoqués :

1) L'UNSP entend l'objectif du SPF Finances de faire du code de déontologie ICT « un instrument d'éducation ». Notre organisation syndicale partage cet objectif et souhaite que des informations et des formations soient dispensées aux agents lors de la mise en œuvre de nouveaux systèmes informatiques (plateforme, logiciel…). Qu'on attire l'attention des agents sur les comportements à adopter et les risques et dangers à éviter. Une sensibilisation semble plus adéquate qu'un texte très restrictif, souvent ressenti comme agressif. Le service communication pourrait agir en support de l'ICT et des managers opérationnels pour atteindre cet objectif.

   Des séances d'information sur ce nouveau code sont-elles prévues ?

   Des formations spécifiques sont-elles prévues ?

   Quelques exemples : Comment crypter des données ; Comment éviter le piratage, pishing ; Comprendre le vocabulaire informatique (logs, pishing, etc.).

Votre correspondant : Aubry MAIRIAUX

Du lundi au vendredi

Rue des Colonies 18-24 Bte 4
1000 BRUXELLES

02/218.16.59

aubry.mairiaux@unsp-finances.be

Des formations spécifiques / ateliers pratiques (mises en situation) à propos de ce code sont-elles prévues ? Cela permettrait d'attirer l'attention des agents sur les comportements à éviter.

2) Combien de temps sont conservés les LOGS ?

3) Par qui ces LOGS seront-ils consultables ?

4) L'UNSP ne peut accepter la suppression de la procédure d'avertissement de l'agent en cas de comportement alarmant (volume de data, temps d'utilisation, etc.). Cela renforce le caractère très coercitif du présent code.

   Nous rappelons deux passages importants du code de 2014 (chapitre 9) qui ont disparu :

   a. *Le SPF Finances s'engage ainsi à garantir le respect du droit fondamental des travailleurs au respect de leur vie privée dans la relation de travail.*

      En matière de logging et d'auditing de ses systèmes, le SPF Finances effectue ainsi les contrôles dans le strict respect des finalités et du principe de proportionnalité.

      Cette partie a été remplacée par le point 1 du chapitre 6. Mais celui-ci nous semble nettement moins explicite, c'est pourquoi nous demandons sa réintégration dans le code.

   b. *Les données de logs sont collectées et traitées en vue du contrôle uniquement si elles sont nécessaires à celui-ci (c'est-à-dire uniquement les données qui, compte tenu de la finalité légitime poursuivie par le contrôle, entraînent l'ingérence la plus réduite dans la sphère privée du travailleur). En vertu du principe de proportionnalité, le contrôle des données de logging ne peut entraîner une ingérence dans la vie privée de l'utilisateur. Si toutefois ce contrôle entraîne une telle ingérence, celle-ci est réduite au minimum indispensable pour effectuer le contrôle.*

      Cette seule suppression suffit elle même à annihiler la thèse d'éducation permanente des agents, mais bien le renforcement sécurité, sanction.

      Nous demandons également la réintégration de ce paragraphe dans le code.

5) Certaines dispositions du code indiquent que l'agent est conscient du fait que l'ICT peut, sans avertir l'agent, contrôler l'utilisation que ce dernier fait de son matériel (PC, smartphone, tablette).

   L'UNSP estime que cette disposition est contraire à la loi.

   Nous demandons que chaque agent soit préalablement averti lors de ce type de contrôle (voir au point 7).

   En outre, nous souhaitons savoir en toute transparence :

   a. Quels sont les comportements qui sont surveillés (quels sont les éléments qui déclenchent cette surveillance ?)

   b. Quels sont les logiciels utilisés pour la surveillance ?

   c. Les agents sont-ils géolocalisés ?

   d. La webcam est-elle utilisée à l'insu de l'agent ?

   e. Le micro est-il utilisé à l'insu de l'agent ?

6) L'UNSP estime que l'utilisateur devrait être averti très précisément :

   a. des procédures de « déclenchement » des divers contrôles et actions possibles ;

   b. du déroulement dudit contrôle ou prélèvement d'informations en temps réel.

Cela permettra d'éviter tout abus et conduire à une meilleure compréhension de la réalité d'audit sous-jacente à la gestion des outils mis à disposition, qui, pour l'instant, est totalement opaque.

Hardenvoort 15 — 2060 Antwerpen
@ : nuod.financien@telenet.be
☏ 0032 – (0)3.226.28.01 🖷 0032 – (0)3/231.11.70
SITE WEB : http://www.nuod-financien.be

Rue des Colonies, 18-24 Bte 4 - 1000 BRUXELLES
@ : unsp.fin@unsp-finances.be
☏ 0032 – (0)2 - 218.16.59
SITE WEB : http://www.unsp-finances.be

7) L'utilisation d'une clé USB est prohibée, sauf autorisation par le service ICT. L'UNSP préférerait que les services ICT forment les agents au cryptage de données. En effet, le transfert de données par WIFI sécurisé n'est pas toujours possible lors d'un contrôle en entreprise.

   Pour ce faire, l'UNSP souhaiterait que soit réintroduit le texte suivant (existant dans le code de déontologie version 2014)

   Le transfert de données sur support externe ne peut être réalisé que dans les conditions suivantes :

   - *Le transport de fichiers professionnels pour usage propre (encryptage obligatoire)*
   - *Le transport de fichiers professionnels dans un contexte de télétravail ou de travail à domicile (encryptage obligatoire)*
   - *Le transfert de fichiers professionnels d'une machine de l'administration à l'autre (encryptage obligatoire)*
   - *L'échange d'information avec des partenaires externes (encryptage recommandé)*
   - *La sauvegarde de certaines données (encryptage obligatoire)*
   - *La sauvegarde de ses données privées. Il est interdit de copier des données professionnelles à titre « privé ».*
   - *Le backup centralisé : procédure automatique de sauvegarde des données des PC sur un serveur central*

   En surplus, l'UNSP encourage le département à développer une plateforme pour que les contribuables et les agents puissent échanger et partager des fichiers de grande taille. En attendant, les clés USB sont souvent la seule solution actuelle possible sur le terrain.

   Cette plateforme est une condition **préalable** nécessaire à la suppression éventuelle de l'utilisation des clés USB.

   Sans une telle plateforme ou une autre solution fiable, selon nous, la suppression de l'utilisation des clefs USB constituerait une entrave importante à l'exercice des missions de nombreux agents.

   Nous souhaitons connaître la position des différentes administrations générales à propos de cette suppression et obtenir les alternatives envisagées.

   Concernant la procédure envisagée pour demander une dérogation à l'exclusion des clés USB (ou disque dur portable), il est indiqué : *Je ne peux sauvegarder, placer ou déposer des données professionnelles sur une clé USB ou un disque dur portable sans l'approbation explicite et préalable du directeur ICT.*

   Quelle sera la procédure ? Comment le directeur ICT va-t-il gérer les demandes – parfois urgentes – des agents (par exemple, en contrôle et qui ont besoin de transférer des données des contribuables) ?

8) Au point 14 du chapitre 1, l'UNSP demande que l'on remplace l'expression « *ne tente pas d'avoir accès* » par « *je ne tente pas de contourner les protections pour avoir accès à… »*.

9) Concernant l'utilisation de l'adresse mail, nous préférons le maintien de la situation actuelle avec un usage mixte raisonné en indiquant « PRIVE » ou « SYND » en fonction des circonstances.

10) En cas d'ATN, l'UNSP demande que les actions privées autorisées soient clairement définies (usage de clé USB, plateforme de stockage, etc.).

11) L'UNSP souhaite également que soit clarifiée la notion « d'usage privé occasionnel ».

12) Trafic internet

    Dans le chapitre 4, au point 5, on peut lire :

Hardenvoort 15 — 2060 Antwerpen
@ : nuod.financien@telenet.be
☏ 0032 – (0)3.226.28.01 🖷 0032 – (0)3/231.11.70
SITE WEB : http://www.nuod-financien.be

Rue des Colonies, 18-24 Bte 4 - 1000 BRUXELLES
@ : unsp.fin@unsp-finances.be
☏ 0032 – (0)2 - 218.16.59
SITE WEB : http://www.unsp-finances.be

Je suis conscient du fait que le Service d'encadrement ICT effectue un audit du trafic internet sur mon lieu de travail. Lorsqu'il est constaté que j'ai commis un abus dans l'utilisation d'internet, ceci peut avoir un impact sur mon évaluation ou le cas échéant aboutir à une mesure disciplinaire.

Pourquoi envisager des sanctions immédiates ? En cas d'abus dans l'utilisation d'Internet, il nous semblerait normal qu'avant de sanctionner, le service ICT prenne contact avec l'agent afin de lui demander des explications et lui fournir éventuellement quelques conseils en matière d'utilisation d'Internet.

13) Chapitre 6 – utilisation des logs et des audits au sein du SPF Finances

On peut y lire :

Le SPF Finances définit les finalités comme suit :

- (…) ;
- le contrôle du temps de travail du personnel du SPF Finances ou de ses prestataires de services ;
- (…).

L'UNSP ne peut accepter que ce contrôle du temps de travail soit inséré dans ce code. C'est totalement contradictoire avec la philosophie de l'horaire variable et ne répond nullement aux objectifs d'un tel code.

D'ailleurs, l'introduction du code précise : *L'utilisation de moyens technologiques peut menacer la sécurité des systèmes d'information et de données (data) du SPF Finances. Cela signifie que toutes les personnes utilisant le hardware, le software ou l'infrastructure ICT mis à disposition par le SPF Finances doivent connaitre et respecter les directives énoncées ci-après.*

Le contrôle du temps de travail ne répond nullement à ces objectifs.

Cet aspect devra être géré et concerté avec le dossier *Mesure de la charge de travail*.

Nous demandons le retrait de ce point.

14) Chapitre 6 – utilisation des logs et des audits au sein du SPF Finances

On peut y lire :

Le SPF Finances définit les finalités comme suit :

- (…) ;
- la production de statistiques en vue d'améliorer la qualité du service.

Pourriez-vous nous communiquer les statistiques concernées et leur finalité ?

15) Traduction

Dans le respect de nos collègues germanophones, ce code sera-t-il traduit en langue allemande ?

Nous restons à votre disposition pour tout renseignement complémentaire.

De plus, l'UNSP souhaiterait pouvoir discuter en surplus :

A. Des difficultés rencontrées par de nombreux agents concernant la connexion via « VPN ALWAYS ON ».

B. L'UNSP souhaiterait savoir si une évaluation de l'utilisation Skype a été réalisée. De nombreux adhérents nous font part de la faible qualité des appels (grésillements fréquents, coupure des mots), de la perte de certains appels, de fonctionnalité qui n'existent plus.

Hardenvoort 15 — 2060 Antwerpen
@ : nuod.financien@telenet.be
☏ 0032 – (0)3.226.28.01 🖷 0032 – (0)3/231.11.70
SITE WEB : http://www.nuod-financien.be

Rue des Colonies, 18-24 Bte 4 - 1000 BRUXELLES
@ : unsp.fin@unsp-finances.be
☏ 0032 – (0)2 - 218.16.59
SITE WEB : http://www.unsp-finances.be

C. Concernant les appareils mis à disposition par le SPF Finances et dont les agents bénéficient d'un ATN, qu'est-il prévu en cas de panne ? Par exemple lorsque l'agent se retrouve sans téléphone ou PC ? Si un appareil de remplacement ne lui est pas attribué, l'ATN pour le mois en cours est-il neutralisé ?

D. Il apparaît que certains agents ont reçu en remplacement un Samsung J6 (en lieu et place du J3). Est-ce le cas pour tous les remplacements ? Est-il prévu que des agents reçoivent des appareils reconditionnés ?

Veuillez recevoir, Monsieur le Président du Comité intermédiaire de concertation en matière de personnel, nos salutations les plus sincères.

Pour l'UNSP - Secteur Finances,

Aubry MAIRIAUX, Président fédéral

Hardenvoort 15 — 2060 Antwerpen
@ : nuod.financien@telenet.be
☏ 0032 – (0)3.226.28.01 🖷 0032 – (0)3/231.11.70
SITE WEB : http://www.nuod-financien.be

Rue des Colonies, 18-24 Bte 4 - 1000 BRUXELLES
@ : unsp.fin@unsp-finances.be
☏ 0032 – (0)2 - 218.16.59
SITE WEB : http://www.unsp-finances.be