AFG
Building the Difference

Directive sur
- l'utilisation et la surveillance du trafic Internet, du courrier électronique et des appels téléphoniques;
- la consultation du compte utilisateur d'un collaborateur.

Le 29 août 2013

Table des matières

Préambule....3
1. Utilisation des services Internet et téléphoniques....3
2. Surveillance des services Internet et téléphoniques....3
2.1 Journalisation....3
2.2 Interdiction des programmes espions....3
2.3 Analyse des journaux....4
2.4 Surveillance dans le cadre de la garantie de la sécurité et du bon fonctionnement du système informatique de l'entreprise....4
2.5 Durée de conservation....4
3. Distinction entre courriels privés et professionnels....4
4. Sanctions en cas d'usage abusif....4
5. Gestion du courrier électronique en cas d'absence / départ d'un collaborateur....5
5.1 Absence prévisible....5
5.2 Absence imprévisible....5
5.3 Absence imprévisible de longue durée....5
5.4 Départ d'un collaborateur....5
6. Consultation du compte utilisateur d'un collaborateur....6
7. Soupçon de comportement punissable....6
8. Informations....6
9. Entrée en vigueur....6
Annexe: formulaire de demande de consultation du compte utilisateur d'un collaborateur....8

AFG
Building the Difference

Préambule

La présente directive permet de déterminer quels collaborateurs des sociétés du Groupe AFG Arbonia-Forster-Holding AG (ci-après «AFG») sont autorisés à utiliser les services Internet et téléphoniques et dans l'affirmative, dans quelles conditions. Par ailleurs, la présente directive a pour objet de protéger les collaborateurs et AFG dans le cadre de la surveillance de ces services ainsi que de la consultation d'un compte d'utilisateur. Les prescriptions locales prévoyant des règles plus strictes ou applicables dans le cadre de la mise en œuvre de la présente directive doivent être respectées.

1. Utilisation des services Internet et téléphoniques

Grâce à un mot de passe personnel, chaque collaborateur a accès aux services Internet (Internet / courriel). L'utilisation de ces services ainsi que des services téléphoniques est destinée en premier lieu à des fins professionnelles et doit permettre au collaborateur d'accomplir son travail de manière plus efficace et/ou plus rationnelle et professionnelle.

L'emploi des services Internet et téléphoniques disponibles doit servir prioritairement aux activités de l'entreprise. L'utilisation de ces services à des fins privées doit être limitée au minimum durant les pauses.

Il est interdit de consulter des sites Web dont les contenus aurait un caractère criminel, pornographique ou raciste. La participation à des activités de cette nature (échanges d'idées par discussion en ligne, e-mail, etc.) est également prohibée. Des filtres automatiques bloquent les contenus de certaines catégories. Toute page présentant les contenus suivants est bloquée pour l'ensemble des collaborateurs: pornographie, activités criminelles, contenus extrémistes, radio Web, discussions en ligne, drogues.

Pour des raisons de sécurité, tous les courriels et accès à Internet (téléchargements incl.) sont automatiquement contrôlés de manière à identifier la présence de virus ou de contenus dangereux et bloqués le cas échéant. Néanmoins, les courriels provenant d'expéditeurs inconnus et ceux faisant référence à des virus dans leur objet doivent être supprimés sans même les ouvrir. Face à des invites sur Internet, il faut toujours répondre par «Non» ou cliquer sur «Annuler». Il est strictement interdit d'ouvrir la moindre pièce jointe d'un courriel provenant d'un expéditeur inconnu.

Toutes les connexions Internet chiffrées (banque en ligne p. ex.) sont déchiffrées et contrôlées automatiquement.

2. Surveillance des services Internet et téléphoniques

2.1 Journalisation

Le département informatique journalise les activités Internet. Les appels téléphoniques entrants et sortants sont journalisés par les opérateurs télécoms. Par journalisation, il faut entendre l'enregistrement en continu d'informations périphériques («qui», «quoi», «quand»). Au sein d'AFG, cette journalisation concerne:

- Internet (pages Internet visitées, utilisateur, date, heure)
- courriels (expéditeur, destinataire, date, heure, objet)
- connexion au système (utilisateur, date, heure)
- téléphone (numéros de téléphone de tous les abonnés, heure, date, durée)

2.2 Interdiction des programmes espions

L'utilisation de programmes espions (ou «spyware») est interdite.

2.3 Analyse des journaux

L'analyse des journaux s'effectue sur différents niveaux:

Analyse anonyme: Cette analyse sert à l'établissement de statistiques, de manière à pouvoir déterminer l'utilisation moyenne d'Internet, les pages Web les plus fréquemment consultées, etc. Les échantillons de personnes analysés doivent toujours être suffisamment étendus pour éviter toute identification d'un collaborateur (tous les collaborateurs d'AFG Management AG, par exemple).

Analyse personnelle: Une analyse personnelle n'est autorisée que si l'analyse anonyme a fait apparaître un usage abusif ou dès lors qu'il y a soupçon en ce sens. Est considérée comme un usage abusif toute violation des conditions d'utilisation spécifiées au chiffre 1 de la présente directive ou d'autres obligations inscrites dans le contrat de travail.

L'analyse personnelle est effectuée à la demande du supérieur hiérarchique et réalisée par le département du personnel compétent, en collaboration avec le département informatique et le responsable de la protection des données, si cette fonction existe. Quand un soupçon d'usage abusif n'est pas corroboré, les analyses personnelles sont immédiatement interrompues et les données recueillies, supprimées.

2.4 Surveillance dans le cadre de la garantie de la sécurité et du bon fonctionnement du système informatique de l'entreprise

Lorsque le système informatique présente une défaillance, malgré les mesures techniques de sécurité, les journaux peuvent être consultés pour en rechercher la cause. Si la cause de la défaillance est liée à un usage abusif, le collaborateur identifié peut être sanctionné conformément au chiffre 4 de la présente directive.

2.5 Durée de conservation

A des fins de preuve, les journaux des activités Internet sont conservés durant quatre semaines, sauf si une éventuelle procédure judiciaire ou de sanction nécessite de les conserver plus longtemps. La conservation des journaux téléphoniques s'effectue conformément aux dispositions locales du droit des télécommunications.

3. Distinction entre courriels privés et professionnels

Le compte e-mail sert en premier lieu les besoins de l'entreprise. Les messages privés doivent être limités au minimum. AFG s'interdit de consulter et/ou de traiter les courriels considérés comme privés. Quand aucun signe extérieur ne permet de faire la distinction entre un courriel privé et professionnel et que la nature d'un courriel ne peut pas être déterminée à la lumière des éléments d'adresse ou d'une quelconque autre manière, AFG est autorisée à considérer que ledit courriel est professionnel. S'il existe des doutes quant à la nature d'un courriel, ils doivent être éclaircis auprès du collaborateur concerné.

Les courriels professionnels peuvent être sécurisés le cas échéant.

Dès qu'il est établi qu'un courriel est de nature privée, AFG n'est pas autorisée à prendre connaissance de son contenu. Cela vaut également en cas de soupçon d'acte punissable par voie d'e-mail ou de tout autre usage abusif selon le chiffre 1.

4. Sanctions en cas d'usage abusif

Si les conditions et règles de surveillance ont été respectées et qu'un abus est révélé, des sanctions peuvent être prises au regard du droit social (blâme, blocage de l'accès à Internet, résiliation, etc.).

Avant toute suppression de fichiers obtenus abusivement, le collaborateur concerné est informé de la chose et il lui est offert la possibilité d'enregistrer les fichiers en question (courriels privés, p. ex.) sur un support de données privé.

5. Gestion du courrier électronique en cas d'absence / départ d'un collaborateur

5.1 Absence prévisible

En cas d'absence d'au moins un jour, le gestionnaire d'absence doit être activé dans Outlook. Dans le message d'absence, le collaborateur concerné doit préciser qui assure la suppléance (avec les coordonnées) pour les questions urgentes et indiquer si les courriels entrants doivent être automatiquement transférés ou non. Le transfert automatique de tous les courriels au suppléant / à la suppléante ne peut être activé que dans des cas exceptionnels.

Si un collaborateur a oublié par mégarde d'activer le gestionnaire d'absence, il y a lieu de procéder comme décrit au chiffre 6.

5.2 Absence imprévisible

En cas d'absence imprévisible (maladie, accident, etc.), le collaborateur s'assure le plus rapidement possible du transfert des courriels entrants urgents. Cela peut se faire par exemple grâce au portail Outlook Web Access (http://service.afg.ch), parfaitement sûr. Le collaborateur peut aussi désigner un suppléant / une suppléante autorisé(e) à lire les courriels entrants et, au besoin, à les traiter. Si le collaborateur n'est pas en mesure de s'occuper du transfert des courriels, il convient de procéder comme décrit au chiffre 6.

5.3 Absence imprévisible de longue durée

Si, dans le cas d'une absence imprévue, la date de retour du collaborateur est impossible à déterminer ou si l'absence dure particulièrement longtemps (plus de 4 semaines), d'autres consultations sont possibles conformément au chiffre 6.

5.4 Départ d'un collaborateur

Le collaborateur sortant est responsable de la restitution de tous les documents professionnels. Il est tenu de nettoyer les lecteurs ainsi que le courrier reçu avant son départ. Les affaires encore en suspens, tels les courriels, ou d'autres informations nécessaires ou utiles à AFG doivent être transmises à qui de droit.

Le collaborateur sortant a la possibilité de supprimer les courriels privés et d'autres documents privés ou encore de les enregistrer sur un support de données privé.

Le compte utilisateur (compte de messagerie incl.) est bloqué au plus tard le dernier jour de travail effectif. Si, après blocage, il s'avère nécessaire de consulter le compte de messagerie ou un dossier de l'utilisateur, ce sont les règles de consultation du chiffre 6 qui s'appliquent. Les expéditeurs qui envoient des courriels à l'adresse e-mail bloquée sont automatiquement informés du fait que l'adresse du destinataire n'est plus opérationnelle. Après concertation avec le supérieur hiérarchique, le gestionnaire d'absence peut être exceptionnellement activé et une adresse e-mail AFG de remplacement peut être spécifiée. Il faut veiller à ce qu'aucune conclusion ne puisse être tirée sur la manière dont il a été mis fin au rapport de travail.

Le compte utilisateur est supprimé 30 jour après le dernier jour de travail effectif, mais au plus tôt à l'expiration du délai de résiliation.

6. Consultation du compte utilisateur d'un collaborateur

Si, malgré les mesures prises au chiffre 5.1 ou encore en cas d'absence imprévue, il s'avère nécessaire de consulter le compte e-mail d'un collaborateur, il faut d'abord prendre contact avec le collaborateur concerné et obtenir son accord pour la consultation. Si celui-ci refuse la consultation ou s'il est injoignable, le supérieur hiérarchique doit transmettre une demande écrite au département du personnel compétent (voir annexe). L'autorisation n'est délivrée que si AFG y a un intérêt supérieur (motifs commerciaux urgents par exemple), qu'il est impossible d'attendre le retour du collaborateur et que toutes les mesures ont été prises pour éviter une consultation. Le transfert automatique de tous les courriels n'est autorisé qu'à titre exceptionnel.

Si la demande est acceptée, le département informatique en est informé et réinitialise le mot de passe. Le supérieur hiérarchique et un collaborateur du département du personnel (principe du double contrôle) participent à la consultation. Le collaborateur absent est informé de la consultation au plus tard le jour de son retour à son poste de travail.

La consultation doit être limitée, en termes de période et de contenu, aux indications figurant dans le formulaire de demande. Seuls les e-mails professionnels peuvent être consultés. Les courriels considérés comme privés ne peuvent être ni ouverts, ni lus, ni déplacés, ni copiés, ni transférés ni supprimés (voir aussi chiffre 3). Le supérieur hiérarchique se transfère à lui-même les courriels nécessaires. Par ailleurs, le gestionnaire d'absence doit être activé et il convient d'indiquer une personne à contacter pour toute affaire urgente.

Les présentes dispositions s'appliquent par analogie après le départ d'un collaborateur et en cas de consultation de dossiers d'un utilisateur.

7. Soupçon de comportement punissable

Si l'analyse des journaux ou d'autres indications prouvent ou suggèrent un comportement punissable, les journaux correspondants sont sécurisés. AFG se réserve le droit de déposer plainte à l'encontre de la personne concernée. Si la consultation de courriels, données, etc. d'ordre privé est nécessaire, la chose ne peut se faire qu'avec l'accord préalable du collaborateur soupçonné. S'il est impossible de demander une autorisation préalable ou si l'autorisation est refusée, l'affaire doit être a priori transmise aux autorités judiciaires compétentes. Dans des cas exceptionnels, AFG peut procéder elle-même à la consultation si un intérêt supérieur et des soupçons concrets le justifient. La consultation s'effectue conformément aux dispositions du chiffre 6 ci-dessus.

AFG s'engage à traiter le résultat des enquêtes effectuées de manière confidentielle à l'égard des tiers, en particulier des autres collaborateurs.

8. Informations

Si vous souhaitez obtenir des informations à propos de la présente directive, vous pouvez vous adresser au Head of Legal & Compliance.

9. Entrée en vigueur

Cette directive entre en vigueur avec effet immédiat.

AFG
Building the Difference

Arbon, le 29 août 2013

AFG Arbonia-Forster-Holding AG

Daniel Frutig
Chief Executive Officer

Andrea Wickart
Head of Legal & Compliance
Secrétaire générale

AFG
Building the Difference

Annexe: formulaire de demande de consultation du compte utilisateur d'un collaborateur

Collaborateur concerné	
Nom:	Société:
Fonction:	
Objet de la consultation	
□ Courriels	□ Fichiers
Motif de la consultation	
□ Absence planifiée	Retour prévu le:
□ Absence non prévue	
□ Le collaborateur a déjà quitté l'entreprise	Départ le:
□ Soupçon de comportement punissable	Motifs concrets du soupçon:
La consultation est nécessaire de toute urgence, parce que	
Etendue de la consultation (informations aussi détaillées que possible)	
Les courriels / fichiers concernant les sujets suivants sont nécessaires de toute urgence:	La recherche de courriels / fichiers doit porter sur la période suivante:
Prise de contact avec le collaborateur concerné	
□ Oui, l'autorisation du collaborateur concerné a été demandée au préalable, avec le résultat suivant:	□ Non, l'autorisation du collaborateur concerné n'a pas été demandée au préalable, parce que:
Alternatives	
Ce qui a été entrepris pour éviter la consultation:	
□ les fichiers nécessaires ont été recherchés dans le répertoire commun (lecteur G: / compte e-mail commun).	□ d'autres membres de l'équipe de la personne absente ont été interrogées sur les fichiers / courriels nécessaires.
□ Divers:	
Lieu et date	**Signature**