Réunion plénière – Le 6/9 – DUPPIGHEIM

Le 22 juin 2018

Réunion thèmes multiples

Compte rendu

Nombre de participants ***: 45.***

Séance ouverte à ***14 h 00.***

Compte rendu et présentations sont complémentaires. Suivre les liens intégrés à ce document.

Sommaire

I. Le C2P : le dispositif pénibilité 2

II. L'évolution de l'OHSAS 18001 vers l'ISO 45001 un nouveau challenge 2

III. Le RGPD contrainte ou opportunité ? 3

IV. Divers 4

Le Président Henri KRUTH souhaite la bienvenue aux participants.

I. Le C2P : le dispositif pénibilité

Me Nathalie KLEIN (FIDAL).

Consulter le diaporama

En 2017, le C3P, « Compte Personnel de Prévention de la Pénibilité » rebaptisé **C2P, « compte professionnel de prévention »** fait l'objet d'un certain nombre d'aménagements.

Le compte professionnel de pénibilité est géré par la CARSAT, il permet d'acquérir 100 points maximum, qui permettront au salarié soit à un départ anticipé en retraite, soit à un droit d'accès à des actions de formation, soit à des réductions de leur temps de travail. Les « ordonnances Macron » favorisent les départ à la retraite, 17 ans d'exposition (en fait 68 trimestres) permettent de partir plus tôt.

Sur le plan réglementaire, il y a toujours 10 facteurs de pénibilité reconnus en matière de prévention, donc à prendre en compte dans le cadre des diagnostics d'exposition et la mise en place des plans d'action ; les données résultantes doivent être consignées en annexe du Document Unique (cf. dias « Les obligations de diagnostic et de prévention »). Le diagnostic est effectué dorénavant par type de poste et non plus par salarié. Les fiches d'exposition ne sont plus à réaliser.

Par contre, seulement 6 facteurs sont retenus dans le C2P pour évaluer les risques d'exposition pour le compte de pénibilité proprement dit :

- le travail de nuit,
- le travail en équipes alternantes,
- le travail répétitif,
- le travail sous températures extrêmes,
- les travaux exercés en milieu hyperbare,
- le bruit.

Ces critères sont pris en considération après application de la prévention, ce qui n'était pas le cas auparavant. L'employeur a obligation dans certaines conditions, de négocier un accord de prévention ou d'établir un plan d'action portant sur 3 des 6 facteurs de risque, plan à la préparation duquel le préventeur doit être associé (cf. dias).

Les 4 facteurs évincés sont :

- les postures pénibles,
- les manutentions de charges manuelles,
- les vibrations mécaniques
- les agents chimiques dangereux.

En contrepartie, un arrêté fixe la liste des maladies professionnelles et des maladies hors tableaux pouvant résulter de ces 4 facteurs et être attestées par la CPAM.

Tous les accords collectifs sont publiés (sauf les licenciements), les accords de confidentialité doivent donc être motivés.

II. L'évolution de l'OHSAS 18001 vers l'ISO 45001 un nouveau challenge

Christophe SCHWARZ (Entreprise Novallia).

Consulter le diaporama

La nouvelle norme européenne ISO 45001 a été éditée en mars 2018, Actuellement on est donc dans une phase de transition avec des retours d'expérience très limités, il serait intéressant de refaire le point dans un an. L'OHSAS ne sera plus valide fin mars 2021. La France n'a pas voté la norme, car le dispositif lui paraît trop lourd pour les PME et TPE et nous disposons du Code du travail, la norme ferait donc double emploi.

Compte tenu du contexte mondial et des chiffres publiés par l'Organisation internationale du travail (un mort toutes les 15 secondes par suite d'un accident du travail) la norme européenne met l'homme au cœur du système !

Elle n'oblige pas à être totalement conforme, mais l'entreprise doit avoir un plan d'action avec des délais établi raisonnablement en fonction des contraintes, notamment économiques et financières.

On retrouve dans l'ISO 45001 la structure « HLS » des normes ISO 9001 et 14001 en dix chapitres s'appuyant sur l'amélioration continue (roue de Deming).

Comme les ISO 9001 et 14001, elle répond à une approche par processus, il est donc fondamental de réaliser une cartographie des processus. La norme elle est certifiante.

Son domaine d'application inclut, dans le domaine de responsabilité de l'entreprise, toutes les activités génératrices de risques qui se trouvent sous son contrôle, produits et services aussi bien internes qu'externes (Entreprises extérieures). C'est la notion de parties intéressées pertinentes pour l'entreprise. L'ensemble doit être intégré dans le système de management SST de l'entreprise et ce, au plus tôt, dès les premiers stades des projets. Un rôle plus important est dévolu à la Direction Par ailleurs, il y a une ouverture vers la QVT.

La **communication** des résultats sécurité doit être interne et externe dorénavant. Un fichier Excel, un diaporama, une photo, etc. sont des **informations documentées, qui** remplacent les procédures et autres formulaires. Les **informations de la base** doivent pouvoir remonter. Ex : on ne peut plus exclure un droit de retrait.

L'Homme est au cœur du système (cité 143 fois dans la norme), les travailleurs doivent être consultés, informés et participer, donc être impliqués dans les processus de décision, cela implique qu'ils soient formés.

Enfin, les normes iso imposent une obligation de résultat pas et non une obligation de moyens.

Q.: Est-ce que la norme intègre les principes généraux de prévention en filigrane ?

R.: Oui complètement !

Q.: Vis-à-vis des entreprises extérieures est-ce que ce n'est pas une situation gênante ?

R.: Les entreprises doivent négocier (ce n'est pas écrit dans le Code du travail) et disposent du plan de prévention ; il doit y avoir échange, ce n'est pas une ingérence.

III. Le RGPD contrainte ou opportunité ?

Éric FLEURIVAL (S^té^ eFLEURIVAL).

Consulter le diaporama

Le Règlement Général de Protection des Données entré en application en Europe le 25 mai 2018, est destiné à protéger les données personnelles susceptibles d'être contenues dans un fichier et s'applique à toute donnée relative à une personne physique, qui peut être identifiée.

En ce qui concerne la Suisse (et les pays non européens) les entreprises sont aussi concernées dans le cadre de ses relations avec des entreprises européennes.

En France la CNIL constitue le relai naturel du RGPD.

Les données sont protégées par défaut : la personne doit donner son accord effectif pour que ses données personnelles soient utilisées, une non réponse équivaut à un refus, c'est le « consentement éclairé ».

L'entreprise détentrice du fichier et ses sous-traitants sont co-responsables de l'utilisation des données un (Entreprise d'expertise comptable concernant les données des salariés par ex).

Sur un plan technique, il est indispensable de s'assurer que l'ensemble des matériels contenant les données est bien sécurisé.

En cas de manquement aux règles, des sanctions pouvant être très importantes sont prévues, amendes pouvant aller jusqu'à 4 % du chiffre d'affaire.

La conformité RGPD offre aux entreprises une véritable opportunité en matière de confiance dans les relations avec les clients et, par conséquent un avantage concurrentiel.

L'entreprise peut avoir une équipe informatique, mais il faut sensibiliser tout le monde

Q.: Les données qui ne servent plus doivent-elles être supprimées ?

R.: Par sécurité, l'entreprise doit veiller à détruire tous les fichiers de données personnelles qui ne sont plus d'actualité, et être vigilant quant aux données contenues sur d'anciens ordinateurs, clés USB, etc.). Quant aux données encore utilisables, les archiver de façon sécurisée.

Q.: Lorsqu'un éditeur met à disposition un logiciel utilisé par une entreprise qui y entre des données personnelles (lors de formations par ex), qui est responsable de ces données ?

R.: Cela fonctionne dans les deux sens. Au cours des relations commerciales si une entreprise est amenée à confier des données de ses clients, elle doit demander à l'entreprise partenaire de faire le nécessaire en matière de protection de ces données. Un suivi doit être mis en place (intégration de mises à jour, etc.). Cela va évoluer, mais concernant les E.-U. par exemple, ce sont d'autres contrats, leur fonctionnement est différent et si on n'accepte pas leurs règles, beaucoup plus souples, il faut changer d'hébergeur.

Q.: Une déclaration à la CNIL doit-elle être faite ?

R.: Non le RGPD annule cette déclaration, c'est le principe de responsabilisation.

Concernant le consentement, pour une association c'est plus simple, en payant sa cotisation l'adhérent accepte implicitement la collecte de ses données personnelles.

Le site de la CNIL est bien documenté, ne pas hésiter à le consulter, il fournit un certain nombre de modèles.

IV. Divers

Henri signale qu'une journée sur les risques routiers professionnels se déroulera à l'APAVE de Weyersheim, le 6 juillet.

Pour notre réunion d'octobre nous n'avons pas de sujet il lance un appel pour nous communiquer des thèmes.

La séance est terminée à 16 h 00.

Le 03/07/2018

Le secrétaire, Jean DUCRET