Comité de sécurité de l'information
Chambres réunies

DELIBERATION N° 22/001 DU 11 JANVIER 2022 RELATIVE A LA COMMUNICATION DE DONNEES A CARACTERE PERSONNEL ENTRE MEDEX ET LES EMPLOYEURS AFFILIES

Vu le Règlement (UE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 *relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE* (règlement général sur la protection des données) ;

Vu la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* ;

Vu la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*, en particulier l'article 114 ;

Vu la loi du 15 août 2012 *relative à la création et à l'organisation d'un intégrateur de services fédéral*, en particulier l'article 35/1, §1, premier, troisième et quatrième paragraphe;

Vu la loi 5 septembre 2018 *instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE*, en particulier les articles 97 et 98 ;

Vu la demande de Medex, du SPF Santé publique ;

Vu le rapport d'auditorat du service public fédéral Soutien et Appui (SPF BOSA) ;

Vu le rapport de M. Daniel HACHE et M. Bart VIAENE;

A. OBJET DE LA DEMANDE

1. L'Administration de l'expertise médicale (Medex) est une institution fédérale relevant du SPF Santé publique, Sécurité de la chaîne alimentaire et Environnement. Il fournit des services aux employeurs en ce qui concerne la gestion:

Les services offerts par Medex aux employeurs sont la gestion :

- du contrôle de l'absentéisme ;
- de la réintégration au travail après une longue période de maladie (prestations réduites) ;
- des accidents du travail ou sur le chemin du travail ;
- des maladies professionnelles ;

• de l'admission à la pension anticipée pour raison médicale pour certaines catégories de travailleurs.

2. Les employeurs concernés par un ou plusieurs de ces services sont principalement:

• Les services publics fédéraux, les services publics fédéraux de programmation, les institutions scientifiques fédérales ;

• Les institutions fédérales d'utilité publique sous personnalité juridique de droit public ;

• Les institutions publiques fédérales de sécurité sociale ;

• Certaines institutions de fonction publique non fédérales ;

• Les organismes et les établissements soumis à l'autorité, au pouvoir de contrôle ou de tutelle du Gouvernement d'une Communauté ou d'une Région (ex : un OIP- organisme d'intérêt public) ou du Collège de la Commission communautaire française qui en fait la demande au Ministre fédéral qui a la Santé publique dans ses attributions;

• Certaines administrations régionales, provinciales, locales ;

• Les zones de secours, la protection civile ;

• D'autres institutions gouvernementales (pouvoir législatif, Cour des comptes, comités I et P).

3. Lors du traitement de données à caractère personnel dans le cadre des services susmentionnés qui sont sollicités par l'employeur, Medex et les employeurs affiliés agissent en tant que responsables du traitement au sens de l'article 4.7 du règlement général sur le traitement des données[1].

4. Dans le cadre de ces services précités fournis par Medex, les données à caractère personnel relatives aux employés concernés sont échangées entre Medex et les institutions affiliées mais également, entre les services des institutions pour un usage interne le plus souvent. En vertu de l'article 20 de la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel*, Medex, en tant qu'organisme du gouvernement fédéral qui communique des données à caractère personnel à un tiers, est tenue de conclure un protocole avec chacun des responsables du traitement destinataires.

5. Medex fournit actuellement à environ 2.200 employeurs affiliés un ou plusieurs des services précités (voy. paragraphe 1).

Pour chaque service qu'il est demandé à Medex de réaliser, il convient de constater que la conclusion et la gestion d'un protocole obligatoire constituent une charge particulièrement lourde pour tous les acteurs concernés.

[1]Règlement (UE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 *relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE* (règlement général sur la protection des données)

Toutefois, lorsqu'une communication de données à caractère personnel est autorisée par une délibération du comité de sécurité de l'information, l'expéditeur des données à caractère personnel est exempté de l'obligation de conclure un protocole avec le destinataire des données à caractère personnel (article 15, paragraphe 5, de la loi du 15 janvier 1990 *relative à la création et à l'organisation d'une banque carrefour de la sécurité sociale* et article 35/1, paragraphe 1, point 8, de la loi du 15 août *20102 portant création et organisation de l'intégrateur de services fédéral*).

6. C'est ainsi que Medex, sur base de cette alternative prévue par la loi, demande au Comité de sécurité de l'information de délibérer une autorisation générale pour l'échange des données à caractère personnel, tenant compte des modalités exposées dans la présente délibération dans le cadre des services qui sont sollicités par ses employeurs affiliés.
Néanmoins, avant que la délibération ne s'applique à l'échange de données à caractère personnel entre Medex et l'employeur concerné , cet employeur affilié est tenu de soumettre auprès de ce même Comité de sécurité de l'information une demande d'adhésion à cette délibération..

7. Étant donné qu'il s'agit de la communication de données personnelles par une institution fédérale à un tiers et, dans certains cas, de la communication de données à caractère personnel aux institutions de sécurité sociale, la demande d'adhésion est soumise aux chambres réunies.

8. La licéité de chaque traitement de données à caractère personnel est reprise au point B2 de la présente délibération avec la référence de la disposition légale qui permet le traitement envisagé. Les différents services fournis par Medex pour lesquels des données à caractère personnel sont les suivants : :

1. La gestion de l'absentéisme

L'agent qui est membre du personnel des administrations de l'Etat est soumis à la surveillance de Medex en ce qui concerne son absence pour raison de maladie (incapacité de travail). La procédure de la gestion des absences pour maladie qui leur est applicable est définie dans les articles 61 et 62 de l'AR du 19 novembre 1998 *relatif aux congés et aux absences accordés aux membres du personnel des administrations de l'Etat*.

1.1. Conditions de déclenchement du traitement

Il s'agit d'absences pour maladie pour lesquelles l'établissement d'un certificat médical est obligatoire, soit :

- Absence pour maladie de plus d'une journée ;
- Absence pour maladie d'une journée, pour autant qu'elle soit au moins la troisième de l'année civile en cours.

1.2. Absence pour maladie avec intervention de Medex

Le travailleur tombe malade.

Le travailleur signale son absence à son employeur.

Le travailleur consulte son médecin traitant, qui établit un certificat médical sur base du modèle légal.

Soit le travailleur envoie directement son certificat médical à Medex (modèle papier) soit le médecin transfère électroniquement le certificat par eMediAtt ;

Medex, dans son recensement des travailleurs absents, procède à la sélection des travailleurs à contrôler.

Ce contrôle peut être initié de différentes manière :

- à la demande éventuelle de l'employeur ;
- sur base du facteur de Bradford, qui évalue l'impact de l'absence sur les opérations de l'employeur ;
- sur sélection statistique.

Un médecin contrôleur est désigné pour chaque travailleur pour lequel un contrôle est requis.

Le médecin mandaté peut consulter le médecin traitant du travailleur qui a été déclaré absent pour raison de maladie.

Sur base de ce contrôle médical, il statue, s

- Sur le bien-fondé de l'absence ;
- Sur le bien-fondé de l'absence, mais en limitant (raccourcissant) la période d'absence ;
- ou encore, sur l'absence de justification médicale et l'annulation de l'absence.

La décision est communiquée immédiatement au travailleur, et un rapport écrit est établi et envoyé au service absentéisme de Medex.

Medex communique à l'employeur la décision consistant en la date de reprise du travail pour le-travailleur concerné.

À la date de reprise, si la maladie le justifie, la procédure est reprise pour prolongation de l'absence.

À la fin du congé de maladie, le travailleur reprend sa fonction.

Le travailleur peut également, si son état de santé le permet, reprendre son service prématurément c'est-à-dire avant la date qui est indiquée sur son certificat médical comme étant la date prévue pour la reprise du travail

1.3. Procédure de recours

La procédure de recours en cas de litige médical, est définie à l'article 63 de l'AR 19/11/1998.

Cette procédure est purement interne à Medex et n'implique pas de transferts de données entre Medex et l'employeur, elle est synthétisée ci-dessous pour complétude du contexte.

Lorsque la décision du médecin contrôleur est contestée par le travailleur, les parties s'entendent sur la désignation d'un médecin-arbitre. En cas de désaccord sur ce point, il est nécessaire de recourir à la liste des médecins-arbitres établie sur base des dispositions de la Loi du 13 juin 1999.

Le médecin arbitre examine le travailleur et statue sur le litige médical. Sa conclusion est transmise à Medex.

2. Gestion de la réintégration au travail après une longue période de maladie (prestations réduites)

La procédure de gestion de la réintégration au travail (prestations réduites pour raisons médicales) est définie dans les articles 50 à 54 de l'AR du 19/11/1998 , ainsi que dans diverses statuts applicables au personnel des services publics non fédéraux.

2.1. Conditions de déclenchement du traitement

L'agent, après une absence pour malade de longue durée (30 jours au moins), peut demander à bénéficier d'une réintégration dans sa fonction en prestations réduites. Cette disposition n'est applicable qu'aux fonctionnaires statutaires.

2.2. Gestion du plan de réintégration au travail

Le travailleur, en fin de période de maladie, décide de demander la réintégration en prestations réduites.

Une demande d'examen médical doit être adressée à Medex, ensuite le travailleur consulte son médecin traitant, qui établit un plan de réintégration, pour trois mois, sur base du modèle légal.

L'examen médical doit avoir lieu au moins 5 jours ouvrables avant la reprise du travail, cet examen porte sur la validation de la première tranche d'un mois du plan de réintégration avec prestations réduites. La personne concernée est avisée immédiatement de la décision.

L'employeur est avisé par Medex de la décision d'accorder ou non le plan, et du taux de prestations.

Les tranches mensuelles suivantes sont également soumises à un examen médical à Medex et la personne concernée et l'employeur sont également avisés des prolongations éventuelles et des conditions de travail à accorder au travailleur.

2.3. Procédure de recours

La procédure de recours en cas de litige médical, est définie à l'article 53 §3 de l'AR 19/11/1998.

Cette procédure est purement interne à Medex et n'implique pas de transferts de données entre Medex et l'employeur, elle est synthétisée ci-dessous pour complétude du contexte.
Lorsque la décision du médecin expert de Medex est contestée par le travailleur, les parties s'accordent sur la désignation d'un médecin-arbitre. En cas de désaccord sur ce point, il est nécessaire de recourir à la liste des médecins-arbitres établie sur base des dispositions de la Loi du 13 juin 1999.

Le médecin arbitre examine le travailleur et statue sur le litige médical. Sa conclusion est transmise à Medex qui la communique à son tour à l'employeur.

3. La gestion des accidents du travail ou sur le chemin du travail

Les procédures de gestion des accidents du travail ou sur le chemin du travail sont définies dans :

- Pour les fonctionnaires fédéraux : l'Arrêté Royal du 24 janvier 1969 relatif à la réparation, en faveur de membres du personnel du secteur public, des dommages résultant des accidents du travail et des accidents survenus sur le chemin du travail, art 7 à 11 ;
- Pour les membres des services de police : Arrêté royal du 30 mars 2001 portant la position juridique du personnel des services de police, partie X, titre III, chapitre III – articles X.III.7 à X.III.30.

Certaines autres catégories de services publics bénéficient, par Arrêtés Royaux, des dispositions de l'AR du 24/01/1969 cité ci-dessus :

- Pour les membres des organismes d'intérêt public : Arrêté Royal du 12 juin 1970 relatif à la réparation, en faveur des membres du personnel des organismes d'intérêt public, des personnes morales de droit public et des entreprises publiques autonomes, des dommages résultant des accidents du travail et des accidents survenus sur le chemin du travail,
- Pour les membres des pouvoir publics locaux : Arrêté Royal du 13 juillet 1970 relatif à la réparation, en faveur de certains membres du personnel des services ou établissements publics du secteur local, des dommages résultant des accidents du travail et des accidents survenus sur le chemin du travail ;

Ces institutions peuvent avoir le choix de désigner un service médical autre que Medex. Si c'est le cas, ces employeurs ne sont pas à prendre en compte pour le bénéfice de la présente demande.

3.1. Conditions de déclenchement du traitement

Le traitement est opéré lorsqu'un travailleur d'un employeur affilié à Medex subit un accident du travail ou un accident sur le chemin du travail, que cet accident occasionne ou non une incapacité de travail.

3.2. Gestion des accidents du travail

Le travailleur touché par l'accident du travail, un ayant droit, son supérieur, ou toute autre personne intéressée, remplit le formulaire de déclaration d'accident. Si une absence au travail de plus d'un jour est (susceptible d'être) occasionnée par l'accident, un certificat médical doit être joint, les documents sont envoyés à l'entité responsable pour la gestion des accidents du travail désignée par l'employeur.

Le responsable de l'employeur déclare l'accident du travail dans Publiato, application gérée par FedRIS (Agence Fédérale des risques professionnels) pour l'échange des données des accidents de travail. Les données du travailleur et de l'employeur sont mises à disposition de Medex au travers de cette application .

Selon le cas, Medex convoque la victime de l'accident et statue sur le lien entre l'accident et l'éventuelle incapacité de travail. Cette décision est communiquée dans les 30 jours à l'employeur :

- Medex peut décider de l'aptitude de la personne à exercer ses fonctions en prestations réduites ;
- Si l'incapacité de travail est de 30 jours au moins, Medex convoque d'office la personne pour déterminer, le cas échéant, le pourcentage d'incapacité permanente ;
- Lorsque la période d'incapacité est inférieure à 30 jours, la personne peut faire établir, par un médecin de son choix, un certificat de guérison sans incapacité de travail ;
- Si la personne estime, sur base d'un rapport médical établi par un médecin de son choix, souffrir d'une incapacité permanente, Medex établit un rapport statuant sur une incapacité permanente ou sur une guérison sans incapacité.

L'employeur (l'autorité) recevant la notification de guérison en fait part au travailleur, qui reprend sa fonction.

Lorsque l'employeur reçoit la notification d'incapacité permanente, il examine :

- Les conditions d'octroi des indemnités ;
- Les éléments du dommage subi.

Sur cette base, il estime si le pourcentage d'incapacité doit être augmenté et propose le paiement d'une rente.

3.3. Procédure de recours

Dans le cas des travailleurs fonctionnaires (AR 24/01/1969, AR 12/06/1970 et AR 13/07/1970), il existe une procédure de recours informelle mise en place par Medex.

Dans le cas des travailleurs de la Police, la procédure est formelle et reprise dans l'AR 30/03/2001, dans le cadre du fonctionnement de l'Office Médico-Légal. (appel aux chambres de recours médical de l'OML).

Ces procédures sont internes à Medex et n'impliquent pas de transferts de données entre Medex et l'employeur.

4. La gestion des maladies professionnelles

Les procédures de gestion des maladies professionnelles sont définies dans :

- Pour les fonctionnaires fédéraux : Arrêté royal du 5 janvier 1971 relatif à la réparation des dommages résultant des maladies professionnelles dans le secteur public ;
- Pour les membres des services de police : Arrêté royal du 30 mars 2001 portant la position juridique du personnel des services de police, partie X, titre III, chapitre III – articles X.III.7 à X.III.30.

4.1. Conditions de déclenchement du traitement

Le traitement est opéré lorsqu'un travailleur d'un employeur affilié à Medex contracte une maladie qui est susceptible de s'être développée en raison du travail et liée aux conditions de travail :

- les maladies professionnelles reconnues comme telles par les lois relatives à la réparation des dommages résultant des maladies professionnelles, coordonnées le 3 juin 1970 (Art. 30 et 30bis) ;
- les maladies professionnelles définies dans les conventions internationales obligatoires pour la Belgique, à partir du jour où ces conventions sont entrées en vigueur en Belgique et conformément à leurs dispositions.

4.2. Gestion des Maladies professionnelles

Le travailleur touché par la maladie professionnelle, un ayant droit, son supérieur, ou toute autre personne intéressée, remplit le formulaire de déclaration. Un certificat médical doit être joint. Les documents sont envoyés à l'entité responsable pour la gestion des maladies professionnelles désignée par l'employeur.

Cette entité responsable communique les documents au Service Evaluation des Dommages Corporels de Medex, par courrier postal ou par tout autre moyen de communication.

Selon le cas, Medex convoque la victime ou transfère la demande d'expertise médicale à FedRIS. Cette expertise reconnaît le caractère professionnel de la maladie et établit le lien entre cette maladie et l'éventuelle incapacité de travail. Sur base des pièces apportées, une décision est prise par Medex.
Lorsque l'employeur reçoit la notification d'incapacité permanente, il examine les conditions d'octroi des indemnités et propose le paiement d'une rente à la victime.

4.3. Procédure de recours

Dans le cas des travailleurs fonctionnaires (AR 05/01/1971), il existe une procédure de recours informelle mise en place par Medex.

Dans le cas des travailleurs de la Police, la procédure est formelle et reprise dans l'AR 30/03/2001, dans le cadre du fonctionnement de l'Office Médico-Légal. (appel aux chambres de recours médical de l'OML).

Ces procédures sont internes à Medex et n'impliquent pas de transferts de données entre Medex et l'employeur.

5. L'admission à la pension anticipée pour raison médicale.

La procédure de mise à la pension prématurée pour cause d'inaptitude physique définitive est définie dans l'AR du 18/08/1939.

Cette admission à la pension anticipée temporaire ou définitive ne peut être prise qu'à l'égard d'un agent statutaire

5.1. Conditions de déclenchement du traitement

L'autorité dont dépend un agent qui est en situation de disponibilité (épuisement des jours de 'capital maladie') pour raison de maladie ou d'accident, ou sujet d'une décision précédente d'inaptitude temporaire pour raison médicale, peut demander à Medex, Service 'Evaluation des capacités de travail' une évaluation de santé dans le but de vérifier l'aptitude de l'agent à assurer sa fonction, et donc potentiellement mettre cet agent en pension prématurée.

5.2. Gestion de la mise en pension anticipée

L'autorité (l'employeur) ou dans certains cas l'agent demande à Medex d'examiner les (in)aptitudes médicales en lien avec la fonction exercée.

Le service Evaluation des capacités de travail convoque l'agent, un médecin non fonctionnaire et un médecin fonctionnaire (du cadre de Medex) pour un examen médical.

L'examen médical a lieu dans un centre médical de Medex proche du domicile de l'agent. Si l'agent n'est pas mobile ou réside à l'étranger, des procédures particulières sont prévue pour l'exécution de cet examen médical.

Le dossier médical est présenté au médecin superviseur qui statue sur l'(in)aptitude de l'agent. Medex transmet à l'agent examiné la décision accompagnée de la motivation médicale. L'agent a alors 30 jours pour introduire un recours ou pour accepter la décision.

La décision est définitive si le délai d'appel des 30 jours est dépassé et que l'agent n'a pas fait pas appel de la décision, si l'agent a accepté la décision ou si la procédure de recours est arrivé à son terme.

L'employeur est uniquement avisé par Medex de la décision définitive concernant son aptitude à exercer ses fonctions (sans communiquer l'annexe 1 de la décision qui contient les aspects médicaux de la déicison). L'employeur est tenu d'exécuter la décision , qui peut être : reprise du travail, inaptitude temporaire, aptitude temporaire à un travail adapté, inaptitude à sa fonction mais aptitude à l'exercice de certaines fonctions, aptitude à un travail adapté, admission temporaire à la pension anticipée, mise à la pension définitive pour cause d'inaptitude médicale définitive.

Les mises en situations temporaires, d'une durée maximale de 24 mois, sont susceptibles d'être révisables, en recommençant la présente procédure. Si l'inaptitude subsiste au terme des 24 mois, elle devient définitive, et la pension anticipée définitive est accordée à l'agent.

5.3. Procédures de recours

La procédure de recours est définie dans l'Arrêté Royal du 7 avril 1995 modifiant l'arrêté royal du 18 août 1939 réglant l'organisation des examens médicaux par le Service de Santé Administratif en lieu et place des commissions provinciales de pensions

Lorsque l'agent conteste la décision de la commission d'aptitude au travail, il transmet les pièces du dossier à son médecin traitant, qui, s'il l'estime nécessaire, remplit le formulaire de recours (délai 30 jours).

Plusieurs voies d'appel sont possibles (consultation avec le médecin fonctionnaire, consultation avec le médecin superviseur, rapport médical circonstancié).

Différents cas de figure pouvant se présenter (accord ou désaccord entre les médecins, fonction de la procédure de recours choisie), il est prévu une procédure d'« arbitrage final » par laquelle un médecin fonctionnaire dirigeant ou son délégué établit la décision finale sur l'(in)aptitude de l'agent à exercer sa fonction.

6. **Echange de données à caractère personnel dans le cadre de la cellule 'customer Database Management'**

La gestion de la 'relation client', opérée par la cellule 'Customer Database Management' est le point central de la gestion des partenaires de Medex, et donc des flux de données organisés avec ses parties prenantes. Les services fournis par Medex aux employeurs et à leurs travailleurs dépendent des 'affiliations' des employeurs aux services offerts par Medex, qu'elles soient obligatoires ou facultatives en fonction du type d'employeur.

6.1 Gestion de la 'relation client'

Deux déclencheurs sont possibles :

• l'employeur se présente spontanément à Medex ;

• un travailleur fait appel à un service de Medex, alors que son employeur n'est pas encore connu de Medex.

L'employeur étant identifié, Medex analyse son statut et en dérive les services possibles qui peuvent lui être offerts.

L'employeur confirme son affiliation aux services auxquels il souhaite recourir.

Medex, sur cette base, configure l'identité de l'employeur dans sa banque de données, et demande à l'ONSS et à la BCSS la consultation des relevés DIMONA (intégration niveau employeur) pour ce nouvel employeur.

L'identification de l'employeur permettra à MEDEX de déterminer qui est son seul et unique interlocuteur représentant l'employeur.

Une première consultation de la liste DIMONA permet de déclarer les travailleurs à la BCSS (intégration niveau personnes). Ces personnes sont également déclarées à FedRIS dans le cadre de l'utilisation du flux de données de Publiato (gestion des accidents du travail).

Les inscriptions « employeur » et « personne » sont confirmées à l'employeur.

Par la suite, les données des personnes sont reprises au travers du réseau BCSS (données RN, publiato, dimona, …) lors de processus de mises à jour automatiques..

Medex dispose des autorisations nécessaires pour la consultation des données via le réseau extranet de la Sécurité Sociale[2].

[2] Arrêté royal du 4 avril 2003 autorisant l'Administration de l'Expertise médicale du Service public fédéral Santé publique, Sécurité de la Chaîne alimentaire et Environnement, à accéder aux informations du Registre national des personnes physiques et à en utiliser le numéro d'identification ; Délibération du CSSS N° 08/006 du 5 février 2008 ; Délibération du CSSS N° 13/050 du 7 mai 2013, modifiée le 2 septembre 2014.

II. TRAITEMENT DE LA DEMANDE

A. COMPETENCE DU COMITE DE SECURITE DE L'INFORMATION

9. La communication de données à caractère personnel par des services publics et des institutions publiques de l'autorité fédérale à des tiers autres que les institutions de sécurité sociale visées à l'article 2, alinéa 1er, 2°, de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale doit faire l'objet une délibération préalable de la chambre autorité fédérale du comité de sécurité de l'information visée dans la loi du 5 septembre 2018 instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en oeuvre du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, dans la mesure où les responsables du traitement de l'instance qui communique et des instances destinatrices ne parviennent pas, en exécution de l'article 20 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, à un accord concernant la communication ou au moins un de ces responsables du traitement demande une délibération et en a informé les autres responsables du traitement. [3]

10. La communication de données à caractère personnel par des services publics et des institutions publiques de l'autorité fédérale à des institutions de sécurité sociale visées à l'article 2, alinéa 1er, 2°, a), de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale doit faire l'objet d'une délibération préalable des chambres réunies du comité de sécurité de l'information, dans la mesure où les responsables du traitement de l'instance qui communique, de l'instance destinatrice et de la Banque-carrefour de la sécurité sociale ne parviennent pas, en exécution de l'article 20 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, à un accord concernant la communication ou au moins un de ces responsables du traitement demande une délibération et en a informé les autres responsables du traitement.[4]

11. La communication de données à caractère personnel par des services publics et des institutions publiques de l'autorité fédérale à des institutions de sécurité sociale visées à l'article 2, alinéa 1er, 2°, b) à f), de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale doit faire l'objet d'une délibération préalable des chambres réunies du comité de sécurité de l'information.[5]

12. Enfin, la chambre de la sécurité sociale et de la santé du comité de sécurité de l'information est chargée d'accorder une autorisation de principe pour toute communication de données à caractère personnel relatives à la santé.[6] Il faut répéter que les données médicales ne peuvent

---

[3] Art. 35/1, §1, premier paragraphe de la loi du 15 août 2012 *relative à la création et à l'organisation d'un intégrateur de services fédéral*.

[4] Art. 35/1, §1, troisième paragraphe de la loi du 15 août 2012 *relative à la création et à l'organisation d'un intégrateur de services fédéral*.

[5] Art. 35/1, §1, quatrième paragraphe de la loi du 15 août 2012 *relative à la création et à l'organisation d'un intégrateur de services fédéral*.

[6] Art. 42, §2, 3° van de wet van 13 december 2006 *houdende diverse bepalingen betreffende gezondheid*.

être traitées uniquement que par Medex ou les médecins qui jouent un rôle dans le processus qui a été enclenché.

L'employeur, en tant que tel, n'a pas accès à ces données, mais bien le service ou la personne qu'il désigne à cet effet, soit pour la gestion des accidents du travail soit pour la gestion des maladies professionnelles (conseiller en prévention médecin du travail ou service de santé administratif).

13. Au vu de ce qui précède, le comité de sécurité de l'information est donc compétent pour statuer sur la communication des données à caractère personnel qui sont mentionnées dans »A. Objet de la demande. Compte tenu du nombre très élevé de destinataires qui seraient concernés, le Comité de sécurité de l'information convient qu'une délibération générale (sous forme, d'une autorisation générale) permettrant aux destinataires visés qui satisfont aux exigences décrites ci-dessous, d'adhérer à cette délibération. Comme indiqué précédemment, toute adhésion à une autorisation générale devra faire obligatoirement l'objet d'une demande d'adhésion préalable de l'employeur introduite auprès du Comité de sécurité de l'information.

B. QUANT AU FOND

B.1. RESPONSABILITE

14. Conformément à l'article 5.2 du Règlement général sur la protection des données (ci-après dénommé «RGPD»), Medex (instance qui a transféré les données) et les employeurs affiliés (instances destinataires) en tant que responsables du traitement sont notamment responsables du respect des principes du RGPD desquels il doivent répondre en cas de responsabilité engagée Leur responsabilité est également engagée si la communication des données à caractère, ayant reçu l'autorisation du Comité de sécurité de l'information, est faite est faite par exemple, à une autre entité, un autre service, ou institution que celui/celle qui a été indiqué dans DIMONA.

Il revient aux responsables du traitement de mettre à jour dans DIMONA la liste des services désignés par l'employeur pour le représenter.

15. Le comité de la sécurité de l'information rappelle que les responsables du traitement doivent tenir un registre des activités de traitement effectuées sous ses responsabilités dans les conditions prévues à l'article 30 du RGPD.

B.2. LICEITE

16. Conformément à l'article 5.1 a) RGPD, les données à caractère personnel doivent être traitées d'une manière licite à l'égard de la personne concernée. Cela signifie que le traitement envisagé doit être fondé sur l'un des motifs juridiques énoncés à l'article 6 RGPD.

17. Le Comité note que le traitement est nécessaire pour s'acquitter d'une obligation légale qui incombe au responsable du traitement (article 6, paragraphe 1, point c), RGPD) en ce qui concerne le traitement de données à caractère personnel dans le cadre de la gestion de l'absentéisme, de la réintégration au travail après une longue période de maladie (prestations réduites), des accidents du travail ou sur le chemin du travail, des maladies professionnelles et de la pension anticipée pour raison médicale ; et que le traitement est nécessaire à l'accomplissement d'une tâche d'intérêt général ou dans l'exercice de l'autorité publique

conférée au responsable du traitement (article 6, paragraphe 1, point e), RGPD) en ce qui concerne la cellule 'customer database management'.

18. Le traitement de données à caractère personnel dans le cadre de la gestion de l'absentéisme

Les principaux textes légaux réglementant les absences du personnel de la fonction publique, qu'ils soient statutaires ou contractuels, ainsi que les contrôles médicaux sont :

• Arrêté Royal du 2/10/1937 portant le statut des agents de l'Etat ;

• Loi du 3 juillet 1978 relative aux contrats de travail ;

• Arrêté royal du 19 novembre 1998 relatif aux congés et aux absences accordés aux membres du personnel des administrations de l'Etat ;

• Loi du 13 juin 1999 relative à la médecine de contrôle.

19. Le traitement de la réintégration au travail après une longue période de maladie (prestations réduites)

Les principaux textes légaux réglementant la réintégration au travail du personnel statutaire de la fonction publique ainsi que les contrôles médicaux y correspondant sont :

• Arrêté Royal du 2/10/1937 portant le statut des agents de l'Etat ;

• Arrêté royal du 19 novembre 1998 relatif aux congés et aux absences accordés aux membres du personnel des administrations de l'Etat ;

• Diverses statuts applicables au personnel des services publics non fédéraux ;

• Loi du 13 juin 1999 relative à la médecine de contrôle.

20. Le traitement de données à caractère personnel dans le cadre de la gestion des accidents du travail ou sur le chemin du travail

Les principaux textes légaux réglementant la réintégration au travail du personnel statutaire de la fonction publique ainsi que les contrôles médicaux y correspondant sont :

• la Loi du 3 juillet 1967 sur la prévention ou la réparation des dommages résultant des accidents du travail, des accidents survenus sur le chemin du travail et des maladies professionnelles dans le secteur public ;

• l'Arrêté Royal du 24 janvier 1969 relatif à la réparation, en faveur de membres du personnel du secteur public, des dommages résultant des accidents du travail et des accidents survenus sur le chemin du travail

• l'Arrêté Royal du 17 septembre 1969 relatif à la réparation, en faveur des membres et du personnel de la Cour des Comptes, des dommages résultant des accidents du travail et des accidents survenus sur le chemin du travail ;

• l'Arrêté Royal du 12 juin 1970 relatif à la réparation, en faveur des membres du personnel des organismes d'intérêt public, des personnes morales de droit public et des entreprises publiques autonomes, des dommages résultant des accidents du travail et des accidents survenus sur le chemin du travail ;

• l'Arrêté Royal du 13 juillet 1970 relatif à la réparation, en faveur de certains membres du personnel des services ou établissements publics du secteur local, des dommages résultant des accidents du travail et des accidents survenus sur le chemin du travail ;

• l'Arrêté royal du 30 mars 2001 portant la position juridique du personnel des services de police ;

• l'Arrêté royal du 11 avril 1975 réorganisant l'Office médico-légal, modifié par les arrêtés royaux des 14 novembre 1991, 7 octobre 2013 et 14 décembre 2018.

21. Le traitement de données à caractère personnel dans le cadre de la gestion des maladies professionnelles

Les principaux textes légaux réglementant la réintégration au travail du personnel statutaire de la fonction publique ainsi que les contrôles médicaux y correspondant sont :

• la Loi du 3 juillet 1967 sur la prévention ou la réparation des dommages résultant des accidents du travail, des accidents survenus sur le chemin du travail et des maladies professionnelles dans le secteur public ;

• l'Arrêté Royal du 5 janvier 1971 relatif à la réparation des dommages résultant des maladies professionnelles dans le secteur public ;

• l'Arrêté royal du 30 mars 2001 portant la position juridique du personnel des services de police ;

• l'Arrêté royal du 11 avril 1975 réorganisant l'Office médico-légal, modifié par les arrêtés royaux des 14 novembre 1991, 7 octobre 2013 et 14 décembre 2018.

22. Le traitement de données à caractère personnel dans le cadre de la gestion de la pension anticipée pour raison médicale

Les principaux textes légaux réglementant la mise à la pension prématurée pour cause d'inaptitude physique définitive du personnel statutaire de la fonction publique ainsi que les contrôles médicaux y correspondant sont :

• Loi du 21 juillet 1844 générale sur les pensions civiles et ecclésiastiques ;

• Loi du 17 février 1849 qui modifie la loi sur les pensions civiles et ecclésiastiques ;

• Arrêté royal du 18 août 1939 réglant l'organisation des examens médicaux par le Service de santé administratif en lieu et place des commissions provinciales des pensions ;

• Loi du 15 mai 1984 portant mesures d'harmonisation dans les régimes de pension, modifiée en dernier lieu par l'arrêté royal du 12 mars 2013 ;

• Loi du 14 février 1961 d'expansion économique, de progrès social et de redressement financier (art. 117) ;

• Arrêté Royal du 20 février 1963 suspendant et réduisant les effets de certaines des règles contenues dans l'art. 117 de la loi du 14 février 1961 d'expansion économique, de progrès social et de redressement financier.

• Loi du 26 juin 1992 portant des dispositions sociales et diverses (art. 134)

23. Le traitement de données à caractère personnel dans le cadre de la cellule 'customer database management'

Le transfert de données à caractère personnel pour les besoins d'affiliation des employeurs est justifié par les dispositions de l'art 6,1, e du RGPD : le transfert de données répond à l'exercice d'une mission d'intérêt public. Ce traitement vient en support et facilite tous les traitements reposant sur une obligation légale exécutée par - et attribuée à - Medex. Le texte légal le plus représentatif de l'importance de ce traitement est l'arrêté Royal du 1ier décembre 2013 *organique de l'Administration de l'expertise médicale*. Ce texte reprend en références tous les textes légaux régissant les activités de Medex, et en fixe les missions.

24. Compte tenu de ce qui précède, le Comité de sécurité de l'information considère que le traitement des données à caractère personnel envisagé est licite.

B.3. LIMITATION DES FINALITES

25. Article 5.1 b) RGPD ne permet le traitement de données à caractère personnel que pour des fins déterminées, explicites et légitimes.

26. Le Comité de sécurité de l'information prend acte du fait que la communication des données à caractère personnel envisagée poursuit les finalités décrites ci-après:

27. Le traitement de données à caractère personnel dans le cadre de la gestion de l'absentéisme

Dans ce cadre, les échanges d'informations entre Medex et les employeurs ont pour but :

• L'enregistrement des informations relatives aux absences des travailleurs et la gestion administrative des justificatifs de ces absences ;

• D'effectuer les contrôles médicaux et évaluer l'(in)aptitude au travail ;

• De mettre à disposition de l'employeur le résultat du contrôle ;

• De vérifier l'effectivité des contrôles médicaux ;

• D'évaluer les impacts des absences pour les employeurs (institutions fédérales) et la fonction publique en général.

28. Le traitement de données à caractère personnel dans le cadre de la gestion de la réintégration au travail après une longue période de maladie (prestations réduites)

Dans ce cadre les échanges d'informations entre Medex et les employeurs ont pour buts :

• L'enregistrement des informations du plan de réintégration ;

• D'effectuer les contrôles médicaux et évaluer la capacité de travail ;

• De mettre à disposition de l'employeur le résultat du/des contrôle(s) ;

• D'exécuter le plan de réintégration.

29. Le traitement de données à caractère personnel dans le cadre de la gestion des accidents du travail ou sur le chemin du travail

Dans ce cadre, les échanges d'informations entre Medex et les employeurs ont pour buts :

• d'établir le rapport médical circonstancié (origine pathologique des lésions invoquées et relation de causalité entre les lésions et les faits invoqués) ;

• de fixer le taux d'invalidité ;

• de remettre un avis à l'Autorité (l'employeur) ;

• d'exécuter l'avis d'accident ;

• de rembourser les frais médicaux ;

• d'examiner les demandes de révision (aggravation ou atténuation) ;

• de réviser le taux d'invalidité.

30. Le traitement de données à caractère personnel dans le cadre de la gestion des maladies professionnelles

Les échanges d'informations entre Medex et les employeurs ont pour buts :

• d'établir le rapport médical circonstancié (origine pathologique des lésions invoquées et relation de causalité entre les lésions et les faits invoqués) ;

• de fixer le taux d'invalidité ;

• de remettre un avis à l'Autorité (l'employeur) ;

• d'exécuter l'avis de maladie ;

• de rembourser les frais médicaux ;

• d'examiner les demandes de révision (aggravation ou atténuation) ;

• de réviser le taux d'invalidité.

31. Le traitement de données à caractère personnel dans le cadre de la gestion de la pension anticipée pour raison médicale

Dans ce cadre, les échanges d'informations entre Medex et les employeurs ont pour buts :

• Évaluer l'(in)aptitude au travail de la personne concernée, en examen ou réexamen ;

• Établir éventuellement une décision de mise en pension prématurée ;

• Communiquer la décision à l'autorité (l'employeur) ;

• Appliquer la décision.

32. Le traitement de données à caractère personnel dans le cadre de la cellule 'customer database management'

Dans ce cadre, les échanges d'informations entre Medex et les employeurs ont pour buts de:

• tenir à jour les listes de clients (administrations/entreprises et personnes physiques, les contrats de travail) ;

• gérer les affiliations des administrations par rapport aux services de Medex ;

• facturer les prestations aux clients payants.

33. Compte tenu de ce qui précède, le comité de sécurité de l'information considère que les finalités du traitement envisagé sont clairement définies, explicitement définies et justifiées.

B.4. PROPORTIONALITE

B.4.1 MINIMISATION DE DONNEES

34. L'article 5.1 b) du RGPD dispose que les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées. Les données à caractère personnel suivantes sont traitées par service fourni:

35. Dans le cadre de la gestion de l'absentéisme les données à caractère personnel suivantes sont communiquées:

- Données d'identification du travailleur : NISS/numéro de registre national, nom, prénom;
- Coordonnées du travailleur : adresses (domicile, résidence, contrôle), numéro de téléphone, adresse mail ;
- Données d'identification employeur : type d'employeur, raison sociale, affiliation ;
- Points de contacts de l'employeur : noms prénoms et fonction des personnes de contact;
- Coordonnées des points de contact : adresses postales, numéros de téléphone, adresses mail ;
- Données des absences : dates de début et de fin de l'absence, type d'absence, sortie autorisée, prolongation ou reprise anticipée, raison de reprise anticipée ;
- Données des contrôles médicaux : statut (exécuté ou non), résultat (absence justifiée ou non) et accord de l'intéressé sur la décision (oui ou non) ;
- Données du certificat : date de réception du certificat, validité du certificat, dates de début et de fin de l'absence couverte par certificat, type d'absence.

Les données médicales sont traitées uniquement par Medex ou les médecins qui jouent un rôle dans le processus. L'employeur n'a pas accès à ces données, sauf lorsque le travailleur les lui communique.

36. Dans le cadre de la gestion de la réintégration au travail après une longue période de maladie (prestations réduites) les données à caractère personnel suivantes sont communiquées:

- Données d'identification du travailleur : NISS/numéro de registre national, nom, prénom
- Coordonnées du travailleur : adresses (domicile, résidence, contrôle), numéro de téléphone, adresse mail
- Données d'identification employeur : type d'employeur, raison sociale, affiliation
- Points de contacts de l'employeur : noms prénoms et fonction des personnes de contact
- Coordonnées des points de contact : adresses postales, numéros de téléphone, adresses mail
- Données des absences : date, durée, prolongation, date de début de la proposition de prestations réduites ;
- Contrôles : type, statut, résultat, appel

37. Dans le cadre de la gestion des accidents du travail ou sur le chemin du travail les données à caractère personnel suivantes sont communiquées:

• Identification personne : NISS/numéro de registre national, nom, prénom;

• Identification médecin : N° INAMI, identité ;

• Coordonnées de la personne : adresse, tél, mail ;

• Coordonnées des prestataires : adresse, tél, mail ;

• Identification des administrations et entreprises : N°BCE, adresses, coordonnées des points de contact, affiliations ;

• Contrats de travail : date début, date de fin, statut ;

• Données de santé (mentale et physique) ;

• Données financières (factures, paiements) ;

• Décision.

Les données médicales sont traitées uniquement par Medex ou les médecins qui jouent un rôle dans le processus. L'employeur n'a pas accès à ces données, mais bien le service ou la personne qu'il désigne pour la gestion des accidents du travail (conseiller en prévention médecin du travail ou service de santé administratif).

38. Dans le cadre de la gestion des maladies professionnelles les données à caractère personnel suivantes sont communiquées:

- Identification personne : NISS/numéro de registre national, nom, prénom;
- Identification médecin : N° INAMI, identité ;
- Coordonnées de la personne : adresse, tél, mail ;
- Coordonnées des prestataires : adresse, tél, mail ;
- Identification des administrations et entreprises : N°BCE, adresses, coordonnées des points de contact, affiliations ;
- Contrats de travail : date début, date de fin, statut ;
- Données de santé (mentale et physique) ;
- Données financières (factures, paiements) ;
- Décision.

Les données médicales sont traitées uniquement par Medex ou les médecins qui jouent un rôle dans le processus. L'employeur n'a pas accès à ces données, mais bien le service ou la personne qu'il désigne pour la gestion des maladies professionnelles (conseiller en prévention médecin du travail ou service de santé administratif).

39. Dans le cadre de la gestion de la pension anticipée pour raison médicale les données à caractère personnel suivantes sont communiquées:

• Données d'identification du travailleur : numéro de registre national (NISS), nom, prénom

• Coordonnées du travailleur : adresses (domicile, résidence, contrôle), numéro de téléphone, adresse mail

• Données relatives à la situation administrative du travailleur : début de la période de maladie, début de la mise en position administrative de disponibilité, fonction auprès de son employeur, examens médicaux auprès du conseiller en prévention-médecin du travail

• Données d'identification employeur : type d'employeur, raison sociale, affiliation

• Points de contacts de l'employeur : noms prénoms et fonction des personnes de contact

• Coordonnées des points de contact : adresses postales, numéros de téléphone, adresses mail

Les données médicales sont traitées uniquement par Medex ou les médecins qui jouent un rôle dans le processus.

L'employeur n'a pas accès à ces données, sauf lorsque c'est le travailleur lui-même, ayant été informé préalablement à cette transmission du traitement de ses données sensibles (p.ex : données relative à sa santé), qui les lui communique (ex ; Annexe 1).

40. Dans le cadre de la collecte des données par la cellule 'customer database management' les données à caractère personnel suivantes sont communiquées et mises à jour régulièrement (en particulier, le service centralisé/décentralisé qui a été désigné dans DIMONA pour représenter l'employeur dans le cadre de la réalisation des tâches confiées au Medex):

• Données d'identification du travailleur : NISS/numéro de registre national, nom, prénom;

• Coordonnées du travailleur : adresse domicile, numéro de téléphone, adresse mail ;

• Données d'identification employeur : N° BCE, type d'employeur, adresses, affiliations ;

• Points de contacts de l'employeur : noms prénoms et fonction des personnes de contact ;

• Coordonnées des points de contact : adresses postales, numéros de téléphone, adresses mail;

• Données de contrats de travail : date de début, date de fin, Dimona ID, n° BCE.

41. Compte tenu des finalités par service fournis telles que décrites aux paragraphes n° 27 à 32, le comité de sécurité de l'information considère que les données à caractère personnel mentionnées sont suffisantes, pertinentes et limitées à ce qui est nécessaire aux fins pour lesquelles elles sont traitées.

B.4.2 LIMITATION DE CONSERVATION

42. Conformément à l'article 5.1 e) du RGPD, les données à caractère personnel doivent être conservées sous une forme qui ne permette pas d'identifier les personnes concernées plus longtemps que nécessaire aux fins pour lesquelles les données à caractère personnel sont obtenues. Medex stocke les données à caractère personnel qu'il traite conformément à la réglementation applicable pendant une période qui a été enregistrée en collaboration avec la les Archives du Royaume comme suit: http://www.arch.be/ViewerJS/?startpage=53#../pdf/fs_web_pub/P4815/EP4815.pdf Les délais en question varient en fonction de la nature des données et du dossier en question. Par exemple, un dossier médical reprenant un cas d'accident du travail ou de maladie professionnelle peut être conservé jusqu'à quelques années après le décès de la personne concernée car il peut toujours y avoir une révision en aggravation, et des ayants-droits peuvent bénéficier d'avantages après le décès de la victime de l'accident du travail ou de la

maladie professionnelle. Afin de pouvoir s'acquitter de leurs obligations en tant qu'employeurs en matière de gestion du personnel et des salaires, les employeurs affiliés (et, en ce qui concerne les données à caractère personnel relatives à la santé, les médecins, les services ou les personnes désignés) devraient pouvoir conserver les données à caractère personnel communiquées par Medex pendant une période appropriée.

En ce qui concerne les données relatives à la gestion des absences pour cause de maladie, à la gestion de la réintégration au travail après une longue période de maladie, à la gestion de la pension anticipée pour raison médicale et à la cellule de gestion de la base de données clients, le comité de sécurité de l'information considère qu'une période de conservation de cinq ans après la cessation de la relation de travail est acceptable.[7]

En ce qui concerne les données relatives à la gestion des accidents du travail ou sur le chemin du travail et des données relatives à la gestion des maladies professionnelles, le comité de sécurité de l'information considère qu'une période de conservation de dix ans après le décès de l'intéressé est acceptable compte tenu de la durée de conservation en vigueur au sein même de Medex.

B.4.3 PERIOCIDITE

43. Le Comité de sécurité de l'information prend note du fait que l'échange entre Medex et ses employeurs affiliés est permanent et quotidien. Les flux de données sont donc effectués en temps réel et ne sont pas limités dans le temps. Étant donné que les prestations fournies par Medex sont effectuées de manière permanente et quotidienne, le Comité de sécurité de l'information considère que ce transfert est justifié. Le Comité note que les objectifs pour lesquels les employeurs affiliés demandent la communication de ces données ne sont pas limités dans le temps et qu'une autorisation pour une durée indéterminée est donc appropriée.

B.4.3 DESTINATAIRES

44. Les données des personnes identifiables ne sont pas transmises à des tiers. Ainsi, les destinataires autorisés des données sont :

• la personne concernée (travailleur) ;

• son employeur ;

• son représentant (médecin traitant, avocat,…) ;

• les institutions de sécurité sociale impliquées dans le traitement concerné ;

• les éventuels sous-traitants de Medex, lors de l'exécution d'un contrat ;

• dans le cadre des maladies professionnelles : l'entité désignée par l'employeur pour la gestion des maladies professionnelles ;

• dans le cadre des accidents du travail : l'entité désignée par l'employeur pour la gestion des accidents du travail.

[7] Cfr. la position de l'Autorité de protection de données : https://www.autoriteprotectiondonnees.be/citoyen/themes/vie-privee-sur-le-lieu-du-travail/donnees-des-travailleurs/dossier-professionnel-

Lorsque des données sont demandées pour des finalités statistiques ou scientifiques, elles sont soit agrégées et analysées par les services de Medex, soit anonymisées avant leur communication au tiers demandeur.

B.5. FORMAT DES DONNEES ET MODALITES DE LA COMMUNICATION

45. Dans le cadre de la gestion de l'absentéisme:

46. Le Comité de sécurité de l'information prend acte du fait que Medex fait largement appel à des techniques informatiques pour le transfert des données. En ce qui concerne spécifiquement la relation Medex-employeurs, une application web 'self-service' à destination des employeurs a été développée. Les certificats médicaux délivrés par les médecins traitants sont repris sous format papier ou transmis directement sous format électronique par le médecin traitant via eMediAtt. Les certificats papier sont en principe envoyés par courrier postal à une boîte postale centrale, ou peuvent exceptionnellement être déposés dans un centre régional de Medex.

47. La relation directe Medex-employeurs est organisée autour d'une application web 'self-service' (application Absentéisme) dont le mode d'emploi est disponible sur le site du SPF santé publique.

Par ailleurs, le SPF santé publique, et en particulier pour Medex, est utilisateur des services de la BCSS en ce qui concerne la consultation de sources authentiques. Entre autres, le Registre National, Publiato, Dimona et la BCE sont consultés régulièrement pour la mise à jour des données signalétiques des employeurs et de leurs travailleurs.

Les certificats médicaux sont en principe déposés dans un centre Medex, envoyés par courrier postal ou transmis directement par le médecin traitant via eMediAtt. L'envoi électronique permet une intégration automatisée des données d'absence des travailleurs dans les banques de données de Medex, alors que les certificats papier doivent être scannés et indexés pour être exploitables sur les plateformes informatiques.

48. Dans le cadre de la gestion de la réintégration au travail après une longue période de maladie (prestations réduites) :

49. Le Comité de sécurité de l'information prend acte du fait que Medex fait largement appel à des techniques informatiques pour le transfert des données. En ce qui concerne spécifiquement la relation Medex-employeurs, une application web 'self-service' à destination des employeurs a été développée (absentéisme, qui gère également les prestations réduites). Les plans de réintégration délivrés par les médecins traitants sont repris sous format papier à Medex et immédiatement scannés. Les certificats papier sont apportés par le travailleur dans un centre régional de Medex lors de ses visites de contrôle de capacité de travail.

50. La relation directe Medex-employeurs est organisée autour d'une application web 'self-service' (application Absentéisme) dont le mode d'emploi est disponible sur le site du SPF santé publique. Par ailleurs, le SPF santé publique, et en particulier pour Medex, est utilisateur des services de la BCSS en ce qui concerne la consultation de sources authentiques. Entre autres, le Registre National, Publiato, Dimona et la BCE sont consultés régulièrement pour la mise à jour des données signalétiques des employeurs et de leurs travailleurs. Les plans de réintégration sont déposés dans un centre Medex au moment de la visite de contrôle, immédiatement scannés et stockés dans une application dédiée.

51. Dans le cadre de la gestion des accidents du travail ou sur le chemin du travail:

Le Comité de sécurité de l'information prend acte du fait que Medex fait largement appel à des techniques informatiques pour le transfert des données. En ce qui concerne la gestion des déclarations d'accidents, une application de FedRIS a été développée pour l'échange de données entre les employeurs et leurs services d'expertise médicale (Publiato). Les formulaires de déclaration d'accidents et les certificats médicaux correspondants, délivrés par les médecins traitants, sont repris sous format papier chez le représentant de l'employeur, et les éléments sont encodés dans Publiato. Chez Medex, tous les documents papier 'entrants' sont immédiatement scannés puis indexés et stockés dans une banque de données documentaire. Medex a également développé une application centrale pour le suivi de tous les dossiers d'expertise médicale (Mediflow) dans laquelle toutes les informations pertinentes des dossiers sont enregistrées.

La relation directe Medex-employeurs est organisée autour de l'application Publiato dont le mode d'emploi est disponible sur le portail de la sécurité sociale. Par ailleurs, le SPF santé publique, et en particulier pour Medex, est utilisateur des services de la BCSS en ce qui concerne la consultation de sources authentiques. Entre autres, le Registre National, Dimona et la BCE sont, parallèlement à Publiato, consultés régulièrement pour la mise à jour des données signalétiques des employeurs et de leurs travailleurs.

52. Dans le cadre de la gestion des maladies professionnelles:

53. Les formulaires de déclaration de maladie professionnelle et les certificats médicaux correspondants, délivrés par les médecins traitants, sont conservés sous format papier chez le représentant de l'employeur, une copie est transmise à Medex, au Service d'Evaluation des Dommages Corporels. En ce qui concerne la gestion des maladies professionnelles, les flux d'information entre les employeurs et Medex ne sont pas encore totalement électronisés. Les documents sont communiqués soit sous forme papier, par courrier postal, soit sous format électronique (scan) par un canal de communication choisi de commun accord (mail avec pièce jointe chiffrée, FedSender, ressource partagée). Chez Medex, tous les documents papier 'entrants' sont immédiatement scannés. Les images des documents sont indexées et stockées dans une banque de données documentaire.Medex a développé une application centrale (Mediflow) pour le suivi de tous les dossiers d'expertise médicale dans laquelle les informations pertinentes des dossiers sont enregistrées.

54. Les dossiers de maladies professionnelles sont marginaux à Medex (107 dossiers MP pour plus de 50.000 traités en 2020). Pour cette raison, les moyens de communication et applications ne sont pas encore totalement intégrés. Au contraire de la gestion des accidents du travail, bien que la base légale soit la même, que les processus soient très similaires - de même que les intervenants (FedRIS), il n'existe pas pour cette matière d'application similaire à Publiato. Ainsi, les dossiers s'échangent de manière 'ad-hoc', et Medex améliore régulièrement son offre de moyens de communication. La majorité des employeurs étant des instances fédérales, il est fait de préférence appel aux moyens de communication centralisés de l'Etat Fédéral (G-Cloud, OneDrive, …). Par ailleurs, le SPF santé publique, et en particulier pour Medex, est utilisateur des services de la BCSS en ce qui concerne la consultation de sources authentiques. Entre autres, le Registre National, Dimona et la BCE sont consultés régulièrement pour la mise à jour des données signalétiques des employeurs et de leurs travailleurs.

55. Dans le cadre de la gestion de la pension anticipée pour raison médicale:

56. Medex fait largement appel à des techniques informatiques pour le transfert des données. Néanmoins, les processus de gestion des pensions prématurées étant complexes et le nombre de demandes relativement faible (environ 10 %), l'informatisation de ce secteur d'activité n'est encore que partiel. Ainsi, la plupart des informations circulent sous forme papier entre Medex et les parties prenantes externes. En interne, les documents sont scannés lors de l'entrée à Medex, sont indexés et stockés sur des serveurs de contenu sécurisés et les informations pertinentes reprises dans des banques de données structurées. Les documents sortants sont générés par des applications informatiques et imprimés puis postés.

57. La communication d'informations entre Medex et l'employeur se fait principalement sous forme papier ou par échange de messages électroniques. Les documents médicaux entrants sont déposés par l'agent dans un centre Medex au moment de la visite de contrôle, immédiatement scannés et stockés dans une application dédiée. Les documents médicaux sortants sont imprimés et postés. Medex étudie la possibilité de créer un formulaire web sécurisé entre l'employeur et ses services.

58. Dans le cadre de dans le cadre de la cellule 'customer database management':

59. Medex fait largement appel à des techniques informatiques pour le transfert des données. En particulier la relation Medex-employeurs, qui consiste en la gestion des listes de travailleurs, est soutenue par une application web 'self-service'. Les informations structurées sont stockées dans différentes bases de données relationnelles qui servent les différents processus métiers de Medex. Les documents papiers entrants sont immédiatement scannés, indexés et stockés dans des banques de données documentaires sécurisées.

60. La majorité des transferts de données entre employeurs et Medex est effectué par le réseau de la BCSS. C'est principalement lors des étapes initiales que les contacts directs avec les employeurs doivent être pris, et souvent par contact personnel. Dans ce cadre, le téléphone et le courriel sont les outils les plus souples, et souvent l'échange d'informations ne contient que peu de données à caractère personnel sensibles.

B.6. DROITS DES PERSONNES CONCERNEES ET TRANSPARENCE

61. Conformément à l'article 14 du règlement général sur la protection des données, le responsable du traitement doit fournir à la personne concernée certaines informations concernant le traitement de données à caractère personnel non obtenues de la personne concernée. Ces informations ne sont pas nécessaires si l'acquisition ou la divulgation des données est expressément prévue par le droit de l'Union ou de l'État membre applicable au responsable du traitement et si ce droit prévoit des mesures appropriées pour protéger les intérêts légitimes de la personne concernée (article 14.5 du RGPD), comme c'est le cas en l'espèce.

62. Le Comité de sécurité de l'information prend acte du fait que Medex n'a pris aucune disposition particulière pour restreindre les droits des personnes concernées, néanmoins la base de licéité de ce traitement (obligation légale) implique que les droits à l'oubli (effacement) et au portage ne sont pas applicables.

63. En ce qui concerne l'accès aux données de santé, pour la consultation du dossier médical, s'il contient des informations concernant la santé mentale p.ex., Medex peut décider que la consultation se fera par l'intermédiaire d'un médecin mandaté par la personne concernée.

64. En ce qui concerne le traitement de données lors des procédures de recours n'implique l'échange de données qu'entre Medex, les médecins experts et la personne concernée (travailleur).

65. Les procédures d'exercice des droits sur les données sont explicitées dans la 'privacy policy' du SPF santé publique, et rappelées sur les formulaires utilisés par Medex. En pratique, il s'agit pour la personne concernée d'adresser sa demande au DPO. Lorsque la personne concernée conteste la façon dont ses droits sont exercés par le SPF, la voie de recours est une plainte à l'Autorité de Protection des Données.

B.7 INTEGRITE ET CONFIDENTIALITE

66. Conformément à l'article 5, paragraphe 1, point f), du RGPD, les données à caractère personnel doivent être traitées de manière à garantir une sécurité appropriée en prenant des mesures appropriées ou organisationnelles, y compris une protection contre les traitements non autorisés ou illicites et contre les pertes, destructions ou dommages accidentels.

67. Conformément à l'article 24 du RGPD, les responsables du traitement doivent tenir compte de la nature, de la portée, du contexte et de la finalité du traitement, ainsi que des différents risques en termes de probabilité et de gravité pour les droits et la liberté des personnes physiques, de prendre les mesures techniques et organisationnelles appropriées pour garantir et démontrer que le traitement est effectué conformément au règlement.

68. Les bases de données et applications de Medex sont hébergées dans l'infrastructure du SPF Santé publique, pour lequel les normes minimales de sécurité de la BCSS sont applicables. Le cadre normatif de BOSA (FISP) et les normes ISO 27k sont également utilisées comme références pour l'amélioration des conditions de sécurité. Il s'agit de, entre autres :

• Site web sécurisé (HTTPS grade A selon Qualys) et authentification forte des utilisateurs externes par e-ID ou ItsMe ;

• Communications de données de sécurité sociale via l'extranet de la sécurité sociale ;

• Le chiffrement des documents digitalisés stockés dans l'infrastructure du SPF ;

• La sécurisation du réseau par firewalls et DMZ ;

• La sécurité physique organisée en barrières physiques concentriques ;

• L'application d'un cadre de sécurité technique commun à l'ensemble de l'infrastructure comprenant : les mises à jour des systèmes, la gestion centralisée des utilisateurs et de leurs droits d'accès, l'authentification des machines dans le réseau, la stratégie de back-ups, la redondance des équipements et l'utilisation de la virtualisation, la gestion des projets de développements et d'acquisitions incluant les aspects sécuritaires, …

69. Aux points de vue des agents et de l'organisation de Medex, les mesures de sécurité sont appliquées en rapport à la sensibilité des données. S'agissant de données de santé, les différentes mesures de sécurité organisationnelles nécessaires sont mises en place :

• Un poste de médecin-surveillant est créé et attribué ;

• Ce médecin dirige le service de la qualité médicale qui surveille l'ensemble des traitements opérés sur les données des patients ;

• Le personnel de Medex, sans exception, est soumis au régime de secret professionnel ; le personnel administratif et infirmier doit remplir et signer un contrat de confidentialité ;

• L'ensemble des sous-traitants (sous-traitants de données, fournisseurs informatiques, matériels,…) sont soumis à contractualisation ;

• les médecins externes sont également sous contrat, et des directives spécifiques concernant les données leur sont fournies, entre autres :

o les informations et données des patients restent la propriété de Medex exclusivement,

o les médecins ne peuvent donc, après leur mission, conserver quelque donnée que ce soit concernant leur expertise ;

• Les projets sont gérés dans Medex par une équipe dédiée sensibilisée à la protection de la vie privée et une attention particulière est accordée à la minimisation et à la qualité des données ;

• Le SPF santé publique dispose d'un service de sécurité de l'information, composé de DPO's qui sont également formés à la sécurité de l'information. Medex dispose par ailleurs d'un correspondant DPO/ chef de projet RGPD qui est en relation permanente avec le service de sécurité du SPF.

70. L'application mise à disposition des employeurs utilise une hiérarchie dans les droits d'accès. Chaque employeur affilié est tenu de désigner un gestionnaire d'accès qui sera responsable de la gestion des comptes locaux (internes à l'employeur). Medex peut recommander certaines mesures de sécurité à l'employeur, par exemple de limiter l'accès à l'application 'absentéisme' à certaines catégories d'utilisateurs. Medex n'a pas d'autres moyens de contrôle chez l'employeur.

71. Les employeurs affiliés qui reçoivent les données à caractère personnel décrites dans le cadre des services fournis par Medex doivent également prévoir les mesures techniques et organisationnelles nécessaires pour protéger les données personnelles contre la destruction non autorisée ou accidentelle, la perte accidentelle et toute altération, accès ou tout autre traitement non autorisé de données à caractère personnel non autorisés. Lors de la demande d'adhésion à cette délibération, les employeurs affiliés devraient donc explicitement indiquer le résultat de l'analyse d'impact sur la protection des données effectuée conformément à l'article 35 du RGPD. Si l'AIPD indique qu'il existe un risque résiduel élevé, le demandeur doit soumettre le traitement prévu à l'autorité chargée de la protection des données, conformément à l'article 36, paragraphe 1, du RGPD.

Par ces motifs,

le Comité de sécurité de l'information, en chambres réunies, decide

que l'échange de données à caractère personnel entre Medex et les employeurs affiliés qui envoient au Comité de sécurité de l'information un engagement écrit et signé[8] de se joindre à cette délibération, est autorisé à condition que les mesures adoptées dans cette délibération pour assurer la protection des données, notamment celles relatives à la limitation des finalités, à la minimisation des données, à la limitation du stockage et à la sécurité de l'information, soient respectées.

En particulier, les bénéficiaires doivent déclarer et, dans la pratique, veiller à ce que:
— le RGPD, la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et toute autre réglementation applicable sont respectées;
— un délégué à la protection des données est désigné;
— un registre des activités de traitement est tenu conformément aux exigences de l'article 30 du RGPD, l'accent étant mis en particulier sur la spécification des finalités concrètes de traitement en référence à toute législation applicable;
— le principe de finalité est respecté, en particulier que les données obtenues ne sont utilisées qu'aux fins décrites dans la présente délibération;
— les données sont supprimées dès qu'elles ne sont plus nécessaires et que la durée maximale de conservation est respectée;
— les données ne sont traitées que par des personnes qui en ont besoin pour l'exercice de leurs fonctions au sein des services mentionnés dans la présente délibération;
— les données ne sont pas divulguées à des tiers, sauf si cette communication est nécessaire dans le cadre d'une poursuite judiciaire ou d'une autre obligation légale;
— si les données sont fournies aux sous-traitants, les dispositions de l'article 28 du RGPD sont respectées, le sous-traitant s'engage à respecter les conditions de cette délibération et à ce que des garanties appropriées soient prévues pour empêcher une utilisation abusive des données. La confidentialité des données devrait être préservée en imposant une obligation de confidentialité à toute personne ayant accès aux données et les données ne devraient pas être divulguées à des tiers.
— les mesures techniques et organisationnelles nécessaires sont prises.

Bart VIAENE
Chambre sécurité sociale et santé

Daniel HACHE
Chambre autorité fédérale

[8] Un modèle de déclaration à utiliser est disponible à l'adresse suivante:
https://dt.bosa.be/fr/csi/autorisations_generales_pour_lautorite_federale

Le siège de la chambre sécurité sociale et santé du comité de sécurité de l'information est établi dans les bureaux de la Banque Carrefour de la sécurité sociale, quai de Willebroeck 38 - 1000 Bruxelles (tél. 32-2-741 83 11) et le siège de la chambre autorité fédérale du comité de sécurité de l'information est établi dans les bureaux du SPF BOSA, boulevard Simon Bolivar 30, 1000 Bruxelles (tél. 32-2-740 80 64).