Comité de sécurité de l'information
Chambre sécurité sociale et santé

CSI/CSSS/23/444

DÉLIBÉRATION N° 17/020 DU 7 MARS 2017, MODIFIÉE LE 6 JUIN 2017, LE 14 JANVIER 2020, LE 6 DÉCEMBRE 2022, LE 7 MARS 2023 ET LE 5 DÉCEMBRE 2023, RELATIVE À LA COMMUNICATION DE DONNÉES À CARACTÈRE PERSONNEL PSEUDONYMISÉES PAR LA BANQUE CARREFOUR DE LA SÉCURITÉ SOCIALE AU SERVICE PUBLIC FÉDÉRAL SÉCURITÉ SOCIALE, EN VUE DE L'ACTUALISATION DU MODÈLE DE MICROSIMULATION POUR LA SÉCURITÉ SOCIALE (MIMOSIS)

Vu la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale*, notamment les articles 5 et 15, § 1er, alinéa 1er;

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

Vu la loi du 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 l'article 97 ;

Vu les demandes du Service public fédéral Sécurité sociale;

Vu les rapports de la Banque Carrefour de la sécurité sociale;

Vu le rapport de monsieur Bart Viaene.

A. OBJET DE LA DEMANDE

1. Le Comité sectoriel de la sécurité sociale et de la santé jadis compétent avait déjà accordé plusieurs autorisations pour le traitement de données à caractère personnel par le service public fédéral Sécurité sociale, dans le cadre de l'exploitation du modèle de microsimulation pour la sécurité sociale (MIMOSIS – *microsimulation model for Belgian social insurance systems*), à savoir par la délibération n° 07/21 du 8 mai 2007 (modifiée à plusieurs reprises), par la délibération n° 09/33 du 2 juin 2009 et par la délibération n° 11/22 du 1er mars 2011. La présente demande a pour objet le traitement de nouvelles données à caractère personnel qui sont disponibles dans le réseau de la sécurité sociale, en vue de l'actualisation du modèle de microsimulation pour la sécurité sociale (car des données à caractère personnel sont entre-temps aussi disponibles pour des *années plus récentes* et pour *davantage de sources*).

2. Ainsi, concernant les intéressés (il s'agit d'environ quatre cent mille individus échantillonnés et leurs membres du ménage), les données à caractère personnel suivantes (en principe pour l'année 2015) seraient mises à la disposition. Les montants seraient toujours exprimés en classes. Les dates seraient exprimées sous la forme de l'année et du mois.

Caractéristiques personnelles: le numéro d'identification pseudonymisé de l'intéressé, de la personne de référence et du ménage, le fait d'être ou non sélectionné lors de l'extraction de l'échantillon, la relation par rapport au chef de ménage, la date de naissance, le pays de naissance, le sexe, la commune du domicile, la première nationalité (en classes), la nationalité actuelle (en classes), le type de ménage, le code LIPRO, l'état civil, le registre d'inscription, le code profession (en cas d'occupation auprès de l'Union européenne), la formation (niveau, forme, réseau, modalités) et le code diplôme.

Situation au 1er janvier 2016 : le registre dans lequel figure l'intéressé, le motif du séjour et le numéro d'identification pseudonymisé des parents et des grands-parents.

Revenus professionnels et allocations (pour tous les trimestres de 2013,2014 et 2015): le salaire brut du travailleur, le salaire brut imposable du travailleur, le revenu indépendant net, l'allocation brute (par institution de sécurité sociale compétente), l'allocation imposable brute (par institution de sécurité sociale compétente), la position sur le marché du travail, le statut en matière de sécurité sociale (par statut possible, l'indication oui/non) et l'intensité de travail au niveau du ménage (selon deux définitions).

Accidents du travail: le pourcentage d'incapacité de travail temporaire/permanente, le pourcentage d'aide de tiers, le début et la fin de l'incapacité de travail, le nombre de jours d'incapacité de travail temporaire avec absence complète/partielle, le salaire perdu, le salaire proposé servant de base de calcul de l'allocation, le montant de l'allocation d'incapacité de travail temporaire avec absence complète/partielle et la catégorie professionnelle au moment de l'accident du travail.

Maladies professionnelles: le pourcentage d'incapacité de travail, le type d'allocation, le salaire de base sur lequel l'allocation est calculée, le type de période, le début et la fin du paiement et le montant de l'allocation.

Autres incapacités de travail: la raison de l'absence, le régime, le nombre de jours d'incapacité de travail, le début et la fin de l'incapacité de travail, le montant de l'allocation, le statut social et la fin de l'emploi en tant que travailleur frontalier.

Interventions d'un centre public d'action sociale: le montant, le début et la fin du paiement, le pourcentage et la description du remboursement par les pouvoirs publics, la réglementation applicable, la catégorie du ménage, le statut, le type, l'acceptation de l'emploi, le type d'emploi, le lieu de travail, l'horaire, le type de programme d'emploi, le type d'organisation intervenant, le type de projet d'intégration individualisé, le type de projet et le type d'activation.

Invalidité et congé de maternité: le code de paiement, le régime, le nombre de jours indemnisés, le montant de l'allocation, le début et la fin de la période de paiement et le début de l'incapacité de travail primaire, le code sortie par régime, le statut social par régime et le code médical par régime (l'affection sur base de laquelle l'intéressé est reconnu comme invalide par le Conseil médical de l'invalidité).

Allocations familiales (régime des travailleurs salariés et régime des travailleurs indépendants, par enfant): le début et la fin du paiement et la qualité de chaque acteur (la relation entre les acteurs peut être retrouvée au moyen du numéro de dossier, de la caisse d'allocations familiales compétente et du bureau compétent).
Activités professionnelles en tant que travailleur indépendant (pour tous les trimestres de 2015): le code profession, le code NACE, la catégorie de cotisations, le code qualité, le début et la fin de l'affiliation et, pour la période 2010-2015, les revenus nets de l'entreprise (par année).

Activités professionnelles en tant que salarié (par ligne d'occupation, pour le quatrième trimestre 2015): le numéro d'identification pseudonymisé de l'employeur, le secteur, le numéro de la commission paritaire, le code travailleur, la classe travailleur (ordinaire/spécifique), l'indice employeur, la catégorie de l'employeur, la classe de dimension, la nature de l'enregistrement (original, réévalué), la raison de l'exclusion, le type de prestation, le pourcentage d'occupation à temps partiel, le pourcentage d'occupation (sans/avec jours assimilés), la prestation principale, le code de réduction, le montant cumulé de la réduction, le montant des cotisations patronales, le montant des cotisations personnelles, le montant de la cotisation spéciale, le nombre de jours rémunérés (temps plein/temps partiel), le nombre de jours rémunérés préavis, le nombre de jours de congé rémunérés, le nombre de jours assimilés rémunérés, le code principal des jours assimilés, le nombre de jours par semaine, le nombre d'heures occupation à temps plein/temps partiel, le nombre d'heures du travailleur de référence, l'équivalent temps plein, l'équivalent temps plein jours assimilés exclus/inclus, le nombre de jours / d'heures prestés (codes de prestation spécifiques), le code de la réduction de cotisation, la base de calcul, le salaire de base, le salaire ordinaire, le salaire d'attente, le salaire forfaitaire, les primes, l'avantage de l'utilisation d'un véhicule, le préavis, l'indemnité de rupture, le salaire journalier calculé, le salaire journalier moyen, la masse salariale soumise aux cotisations, la réduction de cotisations (patronales/personnelles), l'applicabilité du Maribel social, le code cotisations, la base de calcul et le montant des cotisations patronales pour participation aux bénéfices, voitures de société et pensions extralégales et l'arrondissement du lieu de travail.

Activités professionnelles en tant que travailleur (pour chaque année de la période 2006-2015): la classe travailleur, le code cotisations, la raison de l'exclusion, le nombre d'heures d'occupation à temps partiel, le nombre de jours/d'heures assimilés, le nombre de jours/d'heures indemnisés, le nombre de jours rémunérés occupation à temps plein/à temps partiel, le pourcentage d'occupation (sans/avec jours assimilés), l'équivalent temps plein jours assimilés inclus/exclus, les rémunérations sur base annuelle, les rémunérations sur base trimestrielle (en fonction des divers modes de calcul) et le salaire journalier moyen.

Activités professionnelles comme travailleur salarié (pour tous les trimestres de 2015) : la mesure de promotion de l'emploi applicable, l'emploi dans le régime des titres-services et le secteur d'activité principal de l'employeur.

Chômage: le statut de chômage (pour chaque année de la période 2006-2015), le motif (en cas d'interruption de la carrière/de crédit-temps), le montant de l'indemnité journalière octroyée au chômeur, le nombre de jours pour lesquels une allocation de chômage a été perçue, le montant de l'allocation de chômage perçue au cours de l'année, la durée de chômage, le nombre d'heures prestées dans le cadre d'une agence locale de l'emploi au cours de l'année et la catégorie d'indemnisation du chômeur.

Pensions: le code isolé, le code charge de famille, le code conjoint à charge, le nombre d'enfants à charge, le nombre d'autres personnes à charge, la date de début de la pension, la date de prise de cours du droit actuel, le type de droit de pension et le montant brut de la pension.

Statut de personne handicapée (pour tous les trimestres de 2015): le type d'enregistrement, la réglementation applicable, le début et la fin de la procédure de reconnaissance médicale du handicap, la reconnaissance du handicap (50% membres inférieurs, cécité complète, amputation des membres supérieurs, paralysie des membres inférieurs), le pourcentage d'incapacité de l'enfant, le nombre de points obtenus par l'enfant en ce qui concerne l'impact de la maladie (au total et pour chacun des trois piliers séparément: incapacité physique ou mentale, activité et participation, environnement familial), le nombre de points obtenus par l'enfant en ce qui concerne la réduction d'autonomie, la reconnaissance de la réduction de la capacité de gain, le nombre de points obtenus par l'adulte pour la réduction d'autonomie (au total et pour chacun des six critères séparément: possibilités de déplacement, se préparer à manger et manger, hygiène personnelle et s'habiller, entretenir la maison et effectuer du travail domestique, vivre sans surveillance, communication et contact social), la date de décès de la personne concernée, le montant théorique pour la période de paiement, le montant réel payé durant la période de paiement, la classification statistique, le début et la fin de la période de paiement, le montant mensuel simulé total, le montant mensuel simulé de l'allocation d'intégration, le mois par rapport auquel il y a lieu d'indexer, le début et la fin du droit, la date de la décision de révision éventuelle du droit, la date modifiée de la décision, le numéro d'identification codé du partenaire de l'ayant droit, le début et la fin du partenariat et l'indication de l'allocation d'intégration, de l'allocation de remplacement de revenus ou de l'aide aux personnes âgées.

Carrière (SIGEDIS, 1954-2015, par code carrière) : le code carrière, l'année de carrière, la rémunération annuelle, le nombre de jours prestés, le nombre de jours assimilés, le nombre

d'heures par semaine du travailleur de référence, le nombre d'heures prestées en tant que travailleur à temps partiel, le nombre d'heures assimilées, la période d'incapacité de travail (date de début et date de fin), le pourcentage d'incapacité de travail, le droit à l'allocation de garantie de revenus, l'indication selon laquelle l'allocation de garantie de revenus est accordée par mois de l'année, la date de début de maintien des droits, le début et la fin de la période à temps partiel (avec allocation de garantie de revenus), le type d'assujettissement, l'institution de sécurité sociale compétente et le code d'octroi.

B. EXAMEN DE LA DEMANDE

Compétence du Comité de sécurité de l'information

3. En vertu de l'article 5, § 1er, de la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale*, la Banque Carrefour de la sécurité sociale recueille des données à caractère personnel auprès des institutions de sécurité sociale, les enregistre, procède à leur agrégation et les communique aux personnes qui en ont besoin pour la réalisation de recherches pouvant être utiles à la connaissance, à la conception et à la gestion de la protection sociale.

4. Il s'agit, par ailleurs, d'une communication de données à caractère personnel qui, en vertu de l'article 15, § 1er, de la loi du 15 janvier 1990, doit faire l'objet d'une délibération de la chambre sécurité sociale et santé du Comité de sécurité de l'information.

Licéité du traitement

5. Conformément à l'article 6 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,* le traitement n'est licite que si, et dans la mesure où, au moins une des conditions mentionnées à cet article est remplie.

6. La communication des données à caractère personnel pseudonymisées précitées au Service public fédéral Sécurité sociale est légitime au sens de l'article 6, 1, alinéa 1er, c) du RGPD, car elle est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis en vertu de l'article 2, § 1er, 4° en 5°, de l'arrêté royal du 23 mai 2001 *portant création du Service public fédéral Sécurité sociale.*

Principes en matière de traitement de données à caractère personnel

7. En vertu 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,* les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes et elles ne peuvent pas être traitées ultérieurement d'une manière incompatible avec ces finalités (principe de la limitation des finalités), elles doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour

lesquelles elles sont traitées (principe de la minimisation des données), elles doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées (principe de la limitation de la conservation) et elles doivent être traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité).

Limitation de la finalité

8. Le service public fédéral Sécurité sociale souhaite utiliser le modèle de microsimulation pour la sécurité sociale, qui a été enrichi de données à caractère personnel portant sur des années plus récentes et provenant d'un plus grand nombre de sources, pour des études d'appui à la politique. Il s'agit d'une finalité légitime. Cette finalité légitime a déjà été constatée dans le passé par le Comité sectoriel de la sécurité sociale et de la santé jadis compétent (voir supra).

9. Les données à caractère personnel pseudonymisées du réseau de la sécurité sociale seraient notamment utilisées par le Service public fédéral Sécurité sociale pour la réalisation d'études de préparation de la politique en ce qui concerne le cumul de revenus résultant du travail et d'allocations et l'octroi automatique de droits sociaux.

Minimisation des données

10. La chambre sécurité sociale et santé du Comité de sécurité de l'information constate que la communication porte sur un très grand nombre de données à caractère personnel. Elle estime cependant que ces données à caractère personnel, bien qu'elles soient très nombreuses, ne sont pas de nature à donner lieu à une réidentification de la personne concernée, sauf dans le cas d'une connaissance préalable - que l'on ne peut jamais exclure totalement - dans le chef des chercheurs (il s'agit d'une réidentification contextuelle indirecte). Les caractéristiques personnelles proprement dites sont limitées à cet effet et sont généralement communiquées en classes aux chercheurs. Un numéro d'ordre sans signification est par ailleurs attribué à toute personne concernée.

11. Les données à caractère personnel sont communiquées par la Banque Carrefour de la sécurité sociale à un niveau individuel. Le service public fédéral Sécurité sociale doit, en effet, pouvoir déterminer l'impact général de décisions politiques en appliquant ces décisions politiques à un échantillon de cas concrets qui sont représentatifs pour la population belge. Une communication de données anonymes ne suffit pas.

Limitation de la conservation

12. Le service public fédéral Sécurité sociale peut conserver les données à caractère personnel pseudonymisées communiquées aussi longtemps que nécessaire pour leur traitement, dans le cadre de l'exploitation précitée, et ce jusqu'au 31 mars 2024 au plus tard. Passé ce délai, ces données doivent être détruites, sauf en cas de nouvelle délibération du Comité de sécurité de l'information.

Intégrité et confidentialité

13. Le modèle de microsimulation et les données à caractère personnel sont actuellement installés sur des ordinateurs *stand alone* sécurisés par le service public fédéral Sécurité sociale, en vue de leur exploitation. Des tiers peuvent utiliser ces données à caractère personnel à des fins d'exploitation en tant que sous-traitants du service public fédéral Sécurité sociale, mais ce uniquement sur les ordinateurs sécurisés installés au sein du service public fédéral Sécurité sociale.

14. Pour l'instant, MIMOSIS n'est donc accessible qu'au moyen d'ordinateurs en mode *stand alone* sécurisés. Un système d'accès à distance (*remote access*), sur une infrastructure sécurisée, est cependant appelé à remplacer ce mode de travail. Le Service public fédéral Sécurité sociale souhaite cependant que les deux modes de travail (ordinateurs en mode *stand alone* sécurisés et *remote access*) puissent coexister jusqu'à la fin du traitement des données à caractère personnel, prévue le 31 mars 2024. Dans ce cadre, les ordinateurs *stand alone* feraient office de back-up pour le système d'accès à distance.

15. La protection physique et la protection logique du système d'accès à distance et des ordinateurs *stand alone* précités doivent être organisées de sorte à éviter au maximum toute infraction à la réglementation relative à la protection de la vie privée. Le Service public fédéral Sécurité sociale doit par ailleurs utiliser les ordinateurs *stand alone* selon les directives de la Banque Carrefour de la sécurité sociale en matière de protection des ordinateurs.

16. Le Comité de sécurité de l'information constate que cinq collaborateurs du Service public fédéral Sécurité sociale auraient accès aux données à caractère personnel pseudonymisées via le système d'accès à distance et au moyen d'un ordinateur sécurisé. Les données pseudonymisées sont enregistrées sur un support externe chiffré. L'ordinateur n'est pas connecté à l'internet. Les collaborateurs concernés sont tenus de respecter les « *directives visant à protéger les données traitées par ordinateur* » du service de Sécurité de l'information de la Banque Carrefour de la sécurité sociale (voir annexe).

17. Lors de l'utilisation (temporaire) des ordinateurs en mode *stand alone*, les mesures suivantes doivent toujours être appliquées.

- les données à caractère personnel pseudonymisées sont exclusivement conservées sur un système de *remote access* sécurisé et sur deux disques durs externes à titre de copie de sauvegarde ;
- les supports externes sont entièrement chiffrés (« *full disk encryption* ») au moyen de Bitlocker ou Veracrypt et lors de la création d'un mot de passe, les règles suivantes sont appliquées :
  - le mot de passe comporte au moins vingt caractères et contient au moins une minuscule, une majuscule, un chiffre et un caractère spécial ;
  - le mot de passe n'est conservé d'aucune façon sur l'ordinateur *stand alone* et est introduit manuellement à chaque utilisation ;
- le transport du support externe est limité au strict minimum et le support externe n'est jamais placé dans le même sac de transport que l'ordinateur *stand alone* qui permet la lecture des données à caractère personnel pseudonymisées.

18. Par ailleurs, les mesures suivantes sont prises.

- la sécurité des ordinateurs *stand alone* est garantie :
  - il n'y a pas de connexion réseau ou de connexion à internet lorsque l'ordinateur accède au support externe ;
  - sur le disque dur, il n'y a pas de « temp files » qui sont dérivés des informations sécurisées ;
- en ce qui concerne les supports externes :
  - une « *chain of custody* » est prévue (on sait toujours qui a le disque en possession à quel moment) lorsqu'un support externe quitte le bâtiment ;
  - lorsque le disque n'est pas utilisé, celui-ci est rangé en sécurité de sorte qu'il puisse uniquement être obtenu par les personnes autorisées d'y avoir accès ;
  - les données à caractère personnel sur le support sont détruites (ou le support lui-même) lorsqu'elles ne sont plus utilisées.

19. Lors du traitement des données à caractère personnel dans le cadre de l'exploitation du modèle de microsimulation pour la sécurité sociale, il y a lieu de respecter la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale et toute autre réglementation relative à la protection de la vie privée, en particulier le 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* et la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel*.

20. Ainsi, le service public fédéral Sécurité sociale doit, entre autres, veiller au respect de l'article 28 du Règlement précité (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (portant sur la relation entre le responsable du traitement et son sous-traitant).

21. Le service public fédéral Sécurité sociale doit s'engager contractuellement à mettre en œuvre tous les moyens possibles pour éviter une identification des personnes auxquelles les données à caractère personnel pseudonymisées communiquées ont trait.

22. Le service public fédéral Sécurité sociale doit conclure avec les tiers qui interviennent en tant que sous-traitants et qui utilisent les données à caractère personnel, un contrat par lequel ces tiers s'engagent à traiter les données à caractère personnel conformément aux dispositions de la réglementation précitée. A cet égard, il y a lieu d'être très attentif à la description de la finalité précise lors de l'exécution des simulations politiques.

23. Les résultats du traitement ne peuvent pas être publiés sous une forme qui permet l'identification des personnes concernées. Les données à caractère personnel ne peuvent par ailleurs pas être communiquées à des tiers, sauf si le Comité de sécurité de l'information donne explicitement son accord.

Compte tenu de ce qui précède,

la chambre sécurité sociale et santé du comité de sécurité de l'information

conclut que la communication des données à caractère personnel précitées par la Banque Carrefour de la sécurité sociale au Service public fédéral Sécurité sociale, en vue de l'actualisation du modèle de microsimulation pour la sécurité sociale, telle que décrite dans la présente délibération, est autorisée moyennant le respect des mesures de protection des données définies dans la présente délibération.

Bart VIAENE
Président

Annexe : directives visant à protéger les données traitées par ordinateur

Contexte

Lors du traitement de données, les mesures de sécurité sont destinées à garantir au maximum la confidentialité des données traitées. Bien que les ordinateurs offrent en général une protection de base, il est néanmoins recommandé de prévoir une protection supplémentaire des données de sorte à limiter le risque de fuites de données. Le présent document énumère les mesures pertinentes pour la protection des ordinateurs et les mesures supplémentaires de protection des données. Nous partons du principe que les données sont traitées sur un ordinateur destiné à cet effet. Cet ordinateur est appelé un ordinateur « *stand alone* ».

Protection de l'ordinateur

L'ordinateur doit être protégé par des mesures de base. Ces mesures sont notamment :

- un patching régulier du système d'exploitation et des applications utilisées - lorsque l'ordinateur est principalement utilisé en mode off-line, il doit être mis à jour avant de connecter un « *mass storage device* » (MSD) ou un autre support de mémoire mobile ou lorsqu'une connexion réseau est opérée avec des disques ;
- un contrôle d'accès, de sorte que seules les personnes qui ont besoin d'accès à l'ordinateur puissent effectivement y accéder - le mot de passe doit être suffisamment complexe ;
- un dispositif anti-malware actif et actualisé - lorsque l'ordinateur est utilisé principalement en mode off-line, il doit être mis à jour avant de connecter un « *mass storage device* » (MSD) ou un autre support de mémoire mobile ou lorsqu'une connexion réseau est opérée avec des disques ;
- un chiffrement des données sur les supports de données internes (HD, SSD, ...) ;
- un verrouillage (*lock mode*) de l'ordinateur lorsque celui-ci n'est pas utilisé pendant un certain temps ;
- Les connexions externes ne sont pas acceptées, uniquement les sessions lancées à partir du PC.

Les mesures complémentaires suivantes sont prévues pour l'ordinateur *stand alone* :

- désignation d'un responsable pour la gestion des accès.
    - Cette personne sera responsable de l'octroi d'accès aux informations présentes sur le PC, elle veillera à la configuration du PC et à la suppression de l'accès lorsque celui-ci n'est plus nécessaire pour le projet ou lorsque le collaborateur n'est plus actif au sein du projet.
    - A cet effet, le responsable peut faire appel aux départements IT, mais il gardera toujours un aperçu des accès accordés.
    - Le responsable de la gestion des accès veillera à une destruction adéquate des informations lorsque celles-ci ne sont plus nécessaires.

- limitation des applications

    - Seules sont autorisées les applications nécessaires au projet pour lequel les informations sont traitées. Il convient en particulier d'éviter que des programmes permettant de copier ou de transférer des informations soient présents sur l'appareil.

- limitation des accès

    - L'accès à internet doit être désactivé. Les mises à jour de la solution anti-malware, des systèmes d'exploitation et des logiciels doivent être lancées à partir d'un réseau sécurisé.
    - L'accès pour les MSD doit être désactivé. Une exception est cependant possible lorsque des données sécurisées doivent être copiées, mais la fonctionnalité doit ensuite être désactivée.
    - Les utilisateurs disposent de droits minimaux permettant d'exécuter la mission. Des droits d'accès élargis sont uniquement accordés au responsable de la gestion des accès, qui peut déléguer ces droits à la section IT.
    - La section IT peut uniquement accéder à l'ordinateur après autorisation explicite des utilisateurs ou du responsable de la gestion des accès. Cette autorisation peut être obtenue d'un point de vue technique via le réseau sécurisé et sera uniquement accordée pour autant qu'il ne soit pas obtenu accès aux informations. De manière alternative, l'accès du gestionnaire IT peut être limité à un accès physique sous la surveillance de l'utilisateur ou du responsable de la gestion des accès.

- protection complémentaire des données sensibles

    - L'ordinateur est configuré de sorte à ce que les informations sensibles soient mises à la disposition sous forme d'un volume chiffré distinct (supplémentaire) sur le disque dur interne.
    - L'accès à ce volume s'effectue au moyen d'un mot de passe suffisamment complexe et d'un deuxième facteur. Ce deuxième facteur peut être basé sur une clé externe, mais peut également faire appel à un « *key file* » sur le disque dur du PC. La clé externe ou l'information sur le « *key file* » sont uniquement communiquées aux personnes qui ont besoin d'accès aux informations.
    - L'accès à ce volume chiffré ne peut pas avoir lieu lorsque d'autres accès au PC sont en cours. Ainsi, l'accès à internet est interdit à ce moment et il ne sera pas donné accès aux gestionnaires système.
    - Le volume chiffré est déconnecté lorsque le PC est éteint ou lorsque l'utilisateur se déconnecte du PC.
    - Le volume chiffré ne fait pas l'objet d'une copie de sauvegarde.
    - Lorsque l'information n'est plus nécessaire, le volume chiffré est supprimé de sorte à ce qu'il ne puisse pas être récupéré.

- protection physique de l’ordinateur

    - L’ordinateur est uniquement utilisé dans des endroits sûrs.
    - Lorsque le local où le PC est utilisé, est accessible à des personnes autres que l’utilisateur, le PC est attaché au moyen d'un cadenas.
    - La vue sur l’écran doit être limitée de sorte à ce que seuls les utilisateurs puissent consulter les données.
    - Le PC ne peut jamais être laissé sans surveillance. S'il n’est pas utilisé, l'ordinateur doit être rangé dans un endroit sûr.
    - Le transport du PC est à éviter dans toute la mesure du possible. S’il est quand même nécessaire de transporter le PC, l’utilisateur s’assure que toutes les sessions soient clôturées (*log out*) et que le PC soit éteint (*shut down*).

- apport d’informations

    - L'information est traitée selon le concept de « *chain of custody* ». Ceci signifie qu’on sait à tout moment qui dispose des informations.
    - L'information est mise à la disposition du responsable de la gestion des accès sous forme cryptée.
    - Le responsable de la gestion des accès vérifie les mesures de sécurité sur le PC et veille à ce que ces informations soit copiées sur le volume chiffré. A cet égard, il veille à ce qu’aucun fichier temporaire ne soit créé de manière non-sécurisée sur le PC. Aucune information n’est enregistrée dans des fichiers temporaires en dehors du volume chiffré.