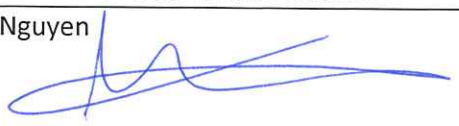
Annexe 1

Fiche de formation RGPD

Titre de la formation	RGPD – Réglementation Générale sur la Protection des Données
Public cible	Personnel assurances du bureau
Objectif(s)	Connaître le règlement et l'appliquer au bureau
Résumé du contenu	Les principes généraux du règlement et comment l'utiliser pratiquement
Forme 1. De type classique (avec présence physique) 2. Enseignement à distance (moyennant protocole de sécurisation, mesurabilité et preuve du suivi) 3. Cours/présentation/exposé	Réunion d'équipe
Matériel de formation (syllabus, slides, livres, documents ...)	Slides fournis par Feprabel
La formation concerne : • les connaissances techniques relatives à la législation et à la gestion d'entreprises, conformément à l'article 270, §1er, 1°, A, a, b, c, e et f, B de la loi du 4 avril 2014 ET/OU • les connaissances techniques relatives aux différentes branches d'assurance, conformément à l'article 270, §1er, 1°, A, d de la loi du 4 avril 2014; • les connaissances techniques relatives à la législation applicable et à la gestion d'entreprises, conformément à l'article 7, § 1er, 1°, A, a, d et B, a, b de l'AR du 1er juillet 2006; • les connaissances techniques relatives aux produits financiers et aux services bancaires et d'investissement, conformément à l'article 7, § 1er, 1°, b et c.	Les connaissances techniques relatives à la législation applicable en matière de RGPD
Planning : Préparation du dernier trimestre 2020, objectifs et chiffres	Date(s): 22/09/2020 Heure de début et de fin de la formation entière: 8h30 – 9h30 Lieu : Agence à Ottignies
Formateur(s)/Orateur(s) (prénom(s) et nom(s)	Audrine Vinaimont et Nicolas Rubbers
Personnes présentes :	Céline Nguyen  Cécile Poulain 

Annexe 2 - Cécile

Procédure concernant les communications électroniques des employés

Article 1 : Courrier électronique

La possibilité d'utiliser le courrier électronique, mise à disposition des employés est exclusivement professionnelle, et ce en tenant compte en particulier du fait que les adresses email des employés comportent le nom de la société. L'employeur accepte toutefois l'usage exceptionnel à des fins privées, à condition que cet usage soit occasionnel, se déroule en-dehors du temps de travail, n'entrave en rien la bonne conduite des affaires de l'entreprise ou la productivité et qu'il ne constitue pas une infraction aux présentes instructions, aux dispositions légales, au contrat de travail ou au règlement de travail. S'il fait usage de cette faculté, l'employé est tenu d'indiquer, dans le sujet du message, que celui-ci a un caractère privé. Il doit en outre supprimer, dans le corps du message, toute mention relative à l'employeur (telle que la signature automatique de l'employeur) et toute autre indication qui pourrait laisser croire à son destinataire que le message est rédigé par l'employé dans le cadre ou à l'occasion de l'exercice de ses fonctions. En aucun cas, le courrier électronique ne pourra être utilisé à l'une des fins prohibées décrites à l'article 3 ci-dessous.

Article 2 : Internet

L'employeur fournit aux employés l'accès à Internet à des fins uniquement professionnelles. En cas d'utilisation d'Internet, les employés doivent respecter les règles suivantes: 1/ L'utilisation d'Internet est en principe limitée à des fins professionnelles ; 2/ L'exploration d'Internet dans une optique d'apprentissage et de développement personnel est toutefois tolérée, mais ne peut en rien porter atteinte au bon fonctionnement du réseau ou à la productivité de l'employé. Elle se fera exclusivement en dehors du temps de travail. L'employeur peut, à tout moment limiter ou interdire cet usage privé ; 3/ L'accès à Internet ne peut se faire qu'en utilisant son propre « accès » (login-name-password). Par conséquent, l'utilisation d'un autre accès n'est pas autorisée sans l'autorisation explicite et écrite du titulaire de cet accès; 4/ L'accès à Internet ne peut être utilisé à des fins prohibées, décrites à l'article 3 ci-dessous; 5/ l'employeur se réserve le droit de bloquer à tout moment et sans avertissement préalable l'accès aux sites dont il juge le contenu illégal, offensant ou inapproprié.

Article 3 : Activités interdites

Il est strictement interdit d'utiliser le système de courrier électronique, l'accès à Internet et, plus généralement, l'infrastructure informatique de l'employeur en vue de: 1/ La diffusion d'informations confidentielles relatives à l'employeur, à ses partenaires commerciaux ou aux travailleurs, sauf dans le cadre strict de la conduite des affaires de l'entreprise; 2/ La diffusion ou le téléchargement de données protégées par le droit de la propriété intellectuelle, en violation des lois applicables; 3/La participation à une activité professionnelle annexe et la recherche du gain ou la poursuite d'un but de lucre; 4/ Transférer des messages électroniques en l'absence de but professionnel légitime, dans des circonstances de nature à porter préjudice à l'employeur ou à l'auteur du message originel; 5/ L'envoi de messages ou la consultation de sites Internet dont le contenu est susceptible de porter atteinte à la dignité d'autrui, notamment l'envoi de messages ou la consultation

de sites à caractère érotique ou pornographique, révisionnistes, prônant la discrimination sur base du sexe, de l'orientation sexuelle, du handicap, de la religion, de la race ou de l'origine nationale ou ethnique, ou des convictions politiques ou religieuses d'une personne ou d'un groupe de personnes; 6/ La participation à des « chaînes de lettres » 7/ Le « spamming » (envoi massif de messages non sollicités); 9/ La participation, au départ de l'infrastructure de l'employeur, à un réseau social, forum de discussion, chat ou newsgroup, quel que soit son sujet en faisant référence à l'employeur ou en émettant des opinions à son sujet 10/ L'achat de biens ou de services aux frais de l'employeur, sans son autorisation préalable et écrite; 11/ L'utilisation de la messagerie électronique ou de l'Internet dans le cadre d'une activité illégale, quelle qu'elle soit.

Cette énumération n'est pas limitative.

Article 4 : Finalités du contrôle de l'utilisation des communications électroniques

L'employeur est attaché au principe du respect de la vie privée des travailleurs sur le lieu de travail. Il exerce toutefois un contrôle de l'usage des techniques de communication électroniques en réseau, dans le respect des dispositions légales applicables, notamment la loi du 8 décembre 1992 et la convention collective de travail n°81 du 26 avril 2002. Les finalités de ce contrôle sont, notamment, les suivantes: 1/ La prévention et la répression de faits illicites ou diffamatoires, de faits contraires aux bonnes moeurs ou susceptibles de porter atteinte à la dignité d'autrui, ainsi que la répression de ces faits; 2/ La protection des intérêts économiques, commerciaux et financiers de l'entreprise, auxquels est attaché un caractère de confidentialité ainsi que la lutte contre les pratiques contraires; 3/ La sécurité et / ou le bon fonctionnement technique des systèmes informatiques en, réseau de l'entreprise, en ce compris le contrôle des coûts y afférents, ainsi que la protection physique des installations de l'entreprise; 4/ Le respect de bonne foi des principes et règles d'utilisation des technologies en réseau, tels que définis par les présentes directives. L'employeur respecte le principe de proportionnalité dans la poursuite de ces finalités.

Article 5 : Mesures de contrôle et d'individualisation

5.1. Mesures de contrôle

5.1.1. Contrôle de l'utilisation d'Internet L'employeur maintient automatiquement une liste générale des sites Internet consultés via le réseau de l'entreprise, indiquant la durée et le moment des visites. Cette liste ne fait pas directement mention de l'identité de l'employé. Elle est régulièrement évaluée par l'employeur. Lorsque, à l'occasion de ce contrôle général ou au départ d'autres sources d'information, l'employeur constate une anomalie, il se réserve le droit, dans le cadre de la poursuite des finalités décrites à l'article 4 ci-dessus, de procéder à l'identification d'un travailleur, conformément à la procédure d'individualisation décrite à l'article 5.2. ci-dessous.

5.1.2. Contrôle du courrier électronique Les messages électroniques sont stockés sur le serveur de l'entreprise pendant une période de douze (12) mois. Les copies de réserves de ces messages sont gardées pendant une période de douze (12) mois. Sur la base d'indices généraux tels la fréquence, le nombre, la taille, les annexes, etc. des messages électroniques, certaines mesures de contrôle pourront être prises par l'employeur vis-à-vis de ces

messages, dans le cadre de la poursuite des finalités décrites à l'article 4 ci-dessus. Si l'employeur considère qu'un usage anormal ou interdit du système de courrier électronique est envisageable, il procédera, dans le cadre de la poursuite des finalités décrites à l'article 4 ci-dessus, à l'identification du travailleur concerné, dans le respect de la procédure d'individualisation décrite à l'article 5.2. ci-dessous.

5.2. Mesures d'individualisation Par « individualisation », on entend le traitement des données collectées lors d'un contrôle en vue de les attribuer à un travailleur identifié ou identifiable.

5.2.1. Individualisation directe L'employeur procédera à une individualisation directe du travailleur s'il suspecte ou a constaté : 2

- La commission de faits illicites ou diffamatoires, de faits contraires aux bonnes mœurs ou susceptibles de porter atteinte à la dignité d'autrui ;
- La violation des intérêts économiques, commerciaux et financiers de l'entreprise, auxquels est attaché un caractère de confidentialité ;
- Une menace à la sécurité et / ou au bon fonctionnement technique des systèmes informatiques en, réseau de l'entreprise, en ce compris le contrôle des coûts y afférents, ainsi que la protection physique des installations de l'entreprise. Le cas échéant, les sanctions appropriées seront prises à l'encontre de ce travailleur, moyennant son audition préalable.

5.2.2. Individualisation indirecte S'il suspecte ou constate un manquement aux présentes directives, l'employeur en avertira l'ensemble des travailleurs par le biais du courrier électronique. En cas de récidive endéans les trois mois, l'employeur identifiera le travailleur qui s'en est rendu coupable et procédera à son audition. Le cas échéant, les sanctions appropriées seront prises à l'encontre de ce travailleur.

Article 6 : Droits du travailleur

Le travailleur dispose des droits d'accès, de rectification, d'effacement, de limitation prévus dans la règlementation sur la protection des données personnelles.

Article 7 : Divers : responsable du traitement

Le responsable du traitement des données de télécommunication en réseau visées par les présentes directives est l'employeur.

Fait à Ottignies, le 22/09/2020

Poulain Cécile

Pour l'employeur

VINAIMONT AUDRINE

L'employée

Annexe 2 - Céline

Procédure concernant les communications électroniques des employés

Article 1 : Courrier électronique

La possibilité d'utiliser le courrier électronique, mise à disposition des employés est exclusivement professionnelle, et ce en tenant compte en particulier du fait que les adresses email des employés comportent le nom de la société. L'employeur accepte toutefois l'usage exceptionnel à des fins privées, à condition que cet usage soit occasionnel, se déroule en-dehors du temps de travail, n'entrave en rien la bonne conduite des affaires de l'entreprise ou la productivité et qu'il ne constitue pas une infraction aux présentes instructions, aux dispositions légales, au contrat de travail ou au règlement de travail. S'il fait usage de cette faculté, l'employé est tenu d'indiquer, dans le sujet du message, que celui-ci a un caractère privé. Il doit en outre supprimer, dans le corps du message, toute mention relative à l'employeur (telle que la signature automatique de l'employeur) et toute autre indication qui pourrait laisser croire à son destinataire que le message est rédigé par l'employé dans le cadre ou à l'occasion de l'exercice de ses fonctions. En aucun cas, le courrier électronique ne pourra être utilisé à l'une des fins prohibées décrites à l'article 3 ci-dessous.

Article 2 : Internet

L'employeur fournit aux employés l'accès à Internet à des fins uniquement professionnelles. En cas d'utilisation d'Internet, les employés doivent respecter les règles suivantes: 1/ L'utilisation d'Internet est en principe limitée à des fins professionnelles ; 2/ L'exploration d'Internet dans une optique d'apprentissage et de développement personnel est toutefois tolérée, mais ne peut en rien porter atteinte au bon fonctionnement du réseau ou à la productivité de l'employé. Elle se fera exclusivement en dehors du temps de travail. L'employeur peut, à tout moment limiter ou interdire cet usage privé ; 3/ L'accès à Internet ne peut se faire qu'en utilisant son propre « accès » (login-name-password). Par conséquent, l'utilisation d'un autre accès n'est pas autorisée sans l'autorisation explicite et écrite du titulaire de cet accès; 4/ L'accès à Internet ne peut être utilisé à des fins prohibées, décrites à l'article 3 ci-dessous; 5/ l'employeur se réserve le droit de bloquer à tout moment et sans avertissement préalable l'accès aux sites dont il juge le contenu illégal, offensant ou inapproprié.

Article 3 : Activités interdites

Il est strictement interdit d'utiliser le système de courrier électronique, l'accès à Internet et, plus généralement, l'infrastructure informatique de l'employeur en vue de: 1/ La diffusion d'informations confidentielles relatives à l'employeur, à ses partenaires commerciaux ou aux travailleurs, sauf dans le cadre strict de la conduite des affaires de l'entreprise; 2/ La diffusion ou le téléchargement de données protégées par le droit de la propriété intellectuelle, en violation des lois applicables; 3/La participation à une activité professionnelle annexe et la recherche du gain ou la poursuite d'un but de lucre; 4/ Transférer des messages électroniques en l'absence de but professionnel légitime, dans des circonstances de nature à porter préjudice à l'employeur ou à l'auteur du message originel; 5/ L'envoi de messages ou la consultation de sites Internet dont le contenu est susceptible de porter atteinte à la dignité d'autrui, notamment l'envoi de messages ou la consultation

de sites à caractère érotique ou pornographique, révisionnistes, prônant la discrimination sur base du sexe, de l'orientation sexuelle, du handicap, de la religion, de la race ou de l'origine nationale ou ethnique, ou des convictions politiques ou religieuses d'une personne ou d'un groupe de personnes; 6/ La participation à des « chaînes de lettres » 7/ Le « spamming » (envoi massif de messages non sollicités); 9/ La participation, au départ de l'infrastructure de l'employeur, à un réseau social, forum de discussion, chat ou newsgroup, quel que soit son sujet en faisant référence à l'employeur ou en émettant des opinions à son sujet 10/ L'achat de biens ou de services aux frais de l'employeur, sans son autorisation préalable et écrite; 11/ L'utilisation de la messagerie électronique ou de l'Internet dans le cadre d'une activité illégale, quelle qu'elle soit.

Cette énumération n'est pas limitative.

Article 4 : Finalités du contrôle de l'utilisation des communications électroniques

L'employeur est attaché au principe du respect de la vie privée des travailleurs sur le lieu de travail. Il exerce toutefois un contrôle de l'usage des techniques de communication électroniques en réseau, dans le respect des dispositions légales applicables, notamment la loi du 8 décembre 1992 et la convention collective de travail n°81 du 26 avril 2002. Les finalités de ce contrôle sont, notamment, les suivantes: 1/ La prévention et la répression de faits illicites ou diffamatoires, de faits contraires aux bonnes moeurs ou susceptibles de porter atteinte à la dignité d'autrui, ainsi que la répression de ces faits; 2/ La protection des intérêts économiques, commerciaux et financiers de l'entreprise, auxquels est attaché un caractère de confidentialité ainsi que la lutte contre les pratiques contraires; 3/ La sécurité et / ou le bon fonctionnement technique des systèmes informatiques en, réseau de l'entreprise, en ce compris le contrôle des coûts y afférents, ainsi que la protection physique des installations de l'entreprise; 4/ Le respect de bonne foi des principes et règles d'utilisation des technologies en réseau, tels que définis par les présentes directives. L'employeur respecte le principe de proportionnalité dans la poursuite de ces finalités.

Article 5 : Mesures de contrôle et d'individualisation

5.1. Mesures de contrôle

5.1.1. Contrôle de l'utilisation d'Internet L'employeur maintient automatiquement une liste générale des sites Internet consultés via le réseau de l'entreprise, indiquant la durée et le moment des visites. Cette liste ne fait pas directement mention de l'identité de l'employé. Elle est régulièrement évaluée par l'employeur. Lorsque, à l'occasion de ce contrôle général ou au départ d'autres sources d'information, l'employeur constate une anomalie, il se réserve le droit, dans le cadre de la poursuite des finalités décrites à l'article 4 ci-dessus, de procéder à l'identification d'un travailleur, conformément à la procédure d'individualisation décrite à l'article 5.2. ci-dessous.

5.1.2. Contrôle du courrier électronique Les messages électroniques sont stockés sur le serveur de l'entreprise pendant une période de douze (12) mois. Les copies de réserves de ces messages sont gardées pendant une période de douze (12) mois. Sur la base d'indices généraux tels la fréquence, le nombre, la taille, les annexes, etc. des messages électroniques, certaines mesures de contrôle pourront être prises par l'employeur vis-à-vis de ces

messages, dans le cadre de la poursuite des finalités décrites à l'article 4 ci-dessus. Si l'employeur considère qu'un usage anormal ou interdit du système de courrier électronique est envisageable, il procédera, dans le cadre de la poursuite des finalités décrites à l'article 4 ci-dessus, à l'identification du travailleur concerné, dans le respect de la procédure d'individualisation décrite à l'article 5.2. ci-dessous.

5.2. Mesures d'individualisation Par « individualisation », on entend le traitement des données collectées lors d'un contrôle en vue de les attribuer à un travailleur identifié ou identifiable.

5.2.1. Individualisation directe L'employeur procédera à une individualisation directe du travailleur s'il suspecte ou a constaté: 2

- La commission de faits illicites ou diffamatoires, de faits contraires aux bonnes moeurs ou susceptibles de porter atteinte à la dignité d'autrui;
- La violation des intérêts économiques, commerciaux et financiers de l'entreprise, auxquels est attaché un caractère de confidentialité;
- Une menace à la sécurité et / ou au bon fonctionnement technique des systèmes informatiques en, réseau de l'entreprise, en ce compris le contrôle des coûts y afférents, ainsi que la protection physique des installations de l'entreprise. Le cas échéant, les sanctions appropriées seront prises à l'encontre de ce travailleur, moyennant son audition préalable.

5.2.2. Individualisation indirecte S'il suspecte ou constate un manquement aux présentes directives, l'employeur en avertira l'ensemble des travailleurs par le biais du courrier électronique. En cas de récidive endéans les trois mois, l'employeur identifiera le travailleur qui s'en est rendu coupable et procédera à son audition. Le cas échéant, les sanctions appropriées seront prises à l'encontre de ce travailleur.

Article 6 : Droits du travailleur

Le travailleur dispose des droits d'accès, de rectification, d'effacement, de limitation prévus dans la règlementation sur la protection des données personnelles.

Article 7 : Divers : responsable du traitement

Le responsable du traitement des données de télécommunication en réseau visées par les présentes directives est l'employeur.

Fait à Ottignies, le 22/09/2020,

Pour l'employeur

VINAIMONT
AUDRINE

L'employé

Annexe 3 - Cécile

Clause de confidentialité

Entre MYASSURANCE.BE SPRL dont le siège social est à l'adresse Avenue des touristes 7 – 1150 Woluwé-Saint-Pierre, représentée par Nicolas Rubbers et Audrine Vinaimont, ci-après l'employeur

Et Poulain Cécile, Rue de Mellery 71 - 1450 Gentinnes, ci-après l'employée.

Il est convenu ce qui suit, qui constitue un avenant au contrat d'emploi qui lie les mêmes parties :

1. Pour permettre à l'employé de mener à bien le travail qui lui est demandé, l'employeur est amené à communiquer à l'employé des données personnelles de tiers (clients, témoins, prospects…) soit verbalement, soit sous forme de documents écrits ou électroniques.
2. L'utilisation de ces données personnelles est soumise à une règlementation stricte et notamment le règlement européen de protection des données personnelles (RGPD) pour lequel l'employeur a mis en place les mesures de sécurité techniques et organisationnelles appropriées. Le respect strict de la confidentialité des données personnelles gérées par l'employeur fait partie intégrante de ces mesures et fait l'objet du présent avenant.
3. L'employeur ne donnera accès à ces données personnelles que si l'employé en a besoin dans l'exercice de son activité professionnelle.
4. Ces informations sont communiquées à l'employé, à charge pour lui de respecter les engagements suivants :

   4.a Garder strictement confidentielles, ne pas publier, ne pas divulguer à des tiers, les données personnelles de quelque nature qu'elles soient qui lui auront été communiquées par l'employeur, qu'elles appartiennent à l'employeur ou à une tierce personne, ou auxquelles il aurait accès ou qui seraient le résultat de ses propres prestations,

   4.b Ne pas utiliser ces données personnelles, directement ou indirectement, pour ses propres besoins autres que la réalisation de la prestation qui lui est demandée.

   4.c Ne communiquer ces données personnelles qu'en fonction des instructions de l'employeur, uniquement à ceux qui auraient besoin de les connaître pour réaliser leurs prestations.

   4.d Ne communiquer ces données à aucun tiers, y compris un sous-traitant de l'employeur, sans instruction de l'employeur

   4.e Ne pas dupliquer les documents (de quelque nature qu'ils soient), remis par l'employeur pour en faire un usage personnel ou en dehors des instructions de l'employeur.

4.f Respecter scrupuleusement les mesures de sécurité techniques et organisationnelles mises en place par l'employeur concernant la protection des données personnelles.

4.g Informer immédiatement l'employeur si l'employé a connaissance d'une divulgation, d'une tentative de divulgation de données personnelles. Dans ce cadre, l'employé prendra toutes les mesures nécessaires à son niveau pour sauvegarder les intérêts de l'employeur.

Fait à Ottignies le 22/09/2020 en deux exemplaires, chaque partie ayant reçu le sien.

Pour l'employeur

L'employée

Annexe 3 - Céline

Clause de confidentialité

Entre MYASSURANCE.BE SPRL dont le siège social est à l'adresse Avenue des touristes 7 – 1150 Woluwé-Saint-Pierre, représentée par Nicolas Rubbers et Audrine Vinaimont, ci-après l'employeur

Et Nguyen Céline, Rue de Bruxelles 26 boite 8 – 1300 Wavre, ci-après l'employé

Il est convenu ce qui suit, qui constitue un avenant au contrat d'emploi qui lie les mêmes parties :

1. Pour permettre à l'employé de mener à bien le travail qui lui est demandé, l'employeur est amené à communiquer à l'employé des données personnelles de tiers (clients, témoins, prospects…) soit verbalement, soit sous forme de documents écrits ou électroniques.
2. L'utilisation de ces données personnelles est soumise à une règlementation stricte et notamment le règlement européen de protection des données personnelles (RGPD) pour lequel l'employeur a mis en place les mesures de sécurité techniques et organisationnelles appropriées. Le respect strict de la confidentialité des données personnelles gérées par l'employeur fait partie intégrante de ces mesures et fait l'objet du présent avenant.
3. L'employeur ne donnera accès à ces données personnelles que si l'employé en a besoin dans l'exercice de son activité professionnelle.
4. Ces informations sont communiquées à l'employé, à charge pour lui de respecter les engagements suivants :

   4.a Garder strictement confidentielles, ne pas publier, ne pas divulguer à des tiers, les données personnelles de quelque nature qu'elles soient qui lui auront été communiquées par l'employeur, qu'elles appartiennent à l'employeur ou à une tierce personne, ou auxquelles il aurait accès ou qui seraient le résultat de ses propres prestations,

   4.b Ne pas utiliser ces données personnelles, directement ou indirectement, pour ses propres besoins autres que la réalisation de la prestation qui lui est demandée.

   4.c Ne communiquer ces données personnelles qu'en fonction des instructions de l'employeur, uniquement à ceux qui auraient besoin de les connaître pour réaliser leurs prestations.

   4.d Ne communiquer ces données à aucun tiers, y compris un sous-traitant de l'employeur, sans instruction de l'employeur

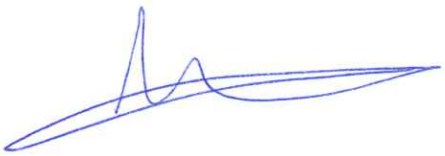
   4.e Ne pas dupliquer les documents (de quelque nature qu'ils soient), remis par l'employeur pour en faire un usage personnel ou en dehors des instructions de l'employeur.

4.f Respecter scrupuleusement les mesures de sécurité techniques et organisationnelles mises en place par l'employeur concernant la protection des données personnelles.

4.g Informer immédiatement l'employeur si l'employé a connaissance d'une divulgation, d'une tentative de divulgation de données personnelles. Dans ce cadre, l'employé prendra toutes les mesures nécessaires à son niveau pour sauvegarder les intérêts de l'employeur.

Fait à Ottignies le 22/09/2020 en deux exemplaires, chaque partie ayant reçu le sien.

Pour l'employeur



L'employé

Annexe 4 - Cécile

Charte informatique de MYASSURANCE.BE SPRL

La présente charte s'applique à l'ensemble des employés de (MYASSURANCE.BE SPRL ci-après dénommé « l'employeur »), ainsi qu'à toute personne, permanente ou temporaire, stagiaire, étudiant, consultant, rémunérée ou non rémunérée, disposant d'un compte de messagerie ou d'un accès au réseau informatique de l'employeur. Dans la présente charte ces personnes seront dénommées « Collaborateurs ».

Chaque collaborateur signera avant de commencer ses activités la présente charte informatique. Un exemplaire lui en sera remis et l'exemplaire signé par lui sera conservé dans son dossier.

Les ressources informatiques (accès au réseau interne, applications, adresse email, accès internet, accès aux données accessibles à partir du réseau, etc.) sont mises à la disposition des collaborateurs dans le cadre de leur activité professionnelle. Si un usage limité à des fins privées est néanmoins autorisé dans le respect de la présente charte, il est recommandé aux collaborateurs d'utiliser leurs outils connectés (smartphones, tablettes ou autres pour leurs usages privés)

Cette charte a pour objet de préciser la responsabilité des collaborateurs, en accord avec la législation belge et européenne, afin d'assurer un usage correct des ressources informatiques, en mettant en place les règles de sécurité techniques et organisationnelles appropriées, pour protéger les données, et en particulier les données personnelles.

Les ressources informatiques sont mises à la disposition des collaborateurs dans le cadre de leur activité professionnelle et, de ce fait, leur usage est réglementé. L'accès aux ressources informatiques et la connexion de tout équipement sur le réseau sont toujours soumis à autorisation, dans le respect des principes suivants :

1. toute autorisation octroyée est strictement personnelle et ne peut, en aucun cas, être cédée, même temporairement, à un tiers
2. l'autorisation est retirée immédiatement en cas de cessation ou de suspension de l'activité pour laquelle elle a été octroyée
3. des restrictions d'accès spécifiques pourront être prévues

L'accès au réseau wifi peut être autorisé exceptionnellement aux clients à qui un code d'accès sera proposé. L'accès au réseau wifi est autorisé pour les collaborateurs de façon limitée pour leur usage privé. Le télétravail, s'il est mis en place, fera l'objet d'un encadrement spécifique.

Le collaborateur ne peut accéder ou tenter d'accéder qu'aux ressources informatiques qui lui sont mis personnellement à sa disposition. Tout collaborateur est responsable de l'usage des ressources informatiques auxquelles il a accès. Il se doit de contribuer, à son niveau, à la sécurité générale de l'entreprise.

Le collaborateur veillera notamment à :

1. renouveler ses login et mots de passe à chaque demande de l'employeur

2. ne pas communiquer son login et mot de passe à des tiers
3. ne pas utiliser ou tenter d'utiliser les comptes d'autrui ni masquer sa véritable identité
4. ne pas tenter de lire, modifier, copier ou détruire des ressources informatiques autres que celles auxquelles l'employeur lui a donné accès
5. ne pas proposer ou rendre accessible aux tiers des données et informations confidentielles, protégées ou non,
6. utiliser les ressources informatiques conformément à la législation en vigueur
7. ne pas introduire de virus dans le système informatique, notamment par le biais de sources douteuses (ouverture d'attachements à des courriers provenant d'inconnus, téléchargement de fichiers issus de sites douteux ou non sécurisés par exemple pas en https)
8. ne pas connecter de périphérique de stockage de masse (clé USB, disque dur externe, carte SD, etc.) sans l'autorisation expresse de l'employeur
9. ne pas installer lui-même aucun logiciel même freeware sur son poste
10. ne pas modifier pas la configuration de son poste ni des applications qu'il utilise
11. respecter scrupuleusement la règlementation sur la protection des données personnelles
12. ne pas procéder à des copies sur tous types de média informatiques en infraction avec les droits de propriété intellectuelle
13. ne pas télécharger ou installer des logiciels ou tout autre contenu soumis à des droits d'auteur sans autorisation expresse de l'employeur
14. ne pas se connecter ni transférer en interne ou vers l'extérieur des contenus illégaux ou contraire aux bonnes mœurs

De plus, si le collaborateur dispose d'un outil mobile appartenant à l'employeur ou s'il bénéficie, moyennant accord express de l'employeur, d'un accès aux ressources informatiques avec ses propres outils connectés, il veillera également :

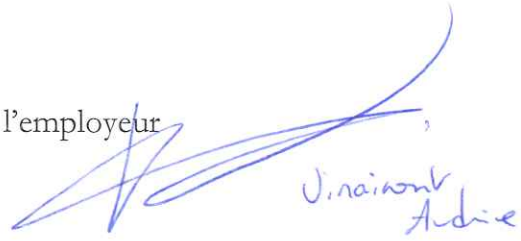
1. à ne jamais laisser seul le PC portable ou l'équipement mobile dans une voiture ou dans un endroit où il serait facilement accessible à des personnes mal intentionnées
2. en cas de perte ou de vol, à avertir immédiatement l'employeur qui bloquera immédiatement les accès aux ressources informatiques
3. à respecter pour ces outils connectés les règles de sécurité énoncées dans la présente charte

Les infractions au contenu de cette charte feront, en fonction de leur gravité, soit l'objet de sanctions telles que celles prévues dans le règlement de travail, soit l'objet de poursuites, pénales ou civiles, suivant la gravité de l'infraction constatée.

Je soussignée, Cécile Poulain, reconnais avoir reçu un exemplaire de la présente, en avoir pris connaissance.

Fait en double exemplaire à Ottignies, le 22/09/2020

Signature de l'employeur



Signature du collaborateur

Annexe 4- Céline.

Charte informatique de MYASSURANCE.BE SPRL

La présente charte s'applique à l'ensemble des employés de (MYASSURANCE.BE SPRL ci-après dénommé « l'employeur »), ainsi qu'à toute personne, permanente ou temporaire, stagiaire, étudiant, consultant, rémunérée ou non rémunérée, disposant d'un compte de messagerie ou d'un accès au réseau informatique de l'employeur. Dans la présente charte ces personnes seront dénommées « Collaborateurs ».

Chaque collaborateur signera avant de commencer ses activités la présente charte informatique. Un exemplaire lui en sera remis et l'exemplaire signé par lui sera conservé dans son dossier.

Les ressources informatiques (accès au réseau interne, applications, adresse email, accès internet, accès aux données accessibles à partir du réseau, etc.) sont mises à la disposition des collaborateurs dans le cadre de leur activité professionnelle. Si un usage limité à des fins privées est néanmoins autorisé dans le respect de la présente charte, il est recommandé aux collaborateurs d'utiliser leurs outils connectés (smartphones, tablettes ou autres pour leurs usages privés)

Cette charte a pour objet de préciser la responsabilité des collaborateurs, en accord avec la législation belge et européenne, afin d'assurer un usage correct des ressources informatiques, en mettant en place les règles de sécurité techniques et organisationnelles appropriées, pour protéger les données, et en particulier les données personnelles.

Les ressources informatiques sont mises à la disposition des collaborateurs dans le cadre de leur activité professionnelle et, de ce fait, leur usage est réglementé. L'accès aux ressources informatiques et la connexion de tout équipement sur le réseau sont toujours soumis à autorisation, dans le respect des principes suivants :

1. toute autorisation octroyée est strictement personnelle et ne peut, en aucun cas, être cédée, même temporairement, à un tiers
2. l'autorisation est retirée immédiatement en cas de cessation ou de suspension de l'activité pour laquelle elle a été octroyée
3. des restrictions d'accès spécifiques pourront être prévues

L'accès au réseau wifi peut être autorisé exceptionnellement aux clients à qui un code d'accès sera proposé. L'accès au réseau wifi est autorisé pour les collaborateurs de façon limitée pour leur usage privé. Le télétravail, s'il est mis en place, fera l'objet d'un encadrement spécifique.

Le collaborateur ne peut accéder ou tenter d'accéder qu'aux ressources informatiques qui lui sont mis personnellement à sa disposition. Tout collaborateur est responsable de l'usage des ressources informatiques auxquelles il a accès. Il se doit de contribuer, à son niveau, à la sécurité générale de l'entreprise.

Le collaborateur veillera notamment à :

1. renouveler ses login et mots de passe à chaque demande de l'employeur

2. ne pas communiquer son login et mot de passe à des tiers
3. ne pas utiliser ou tenter d'utiliser les comptes d'autrui ni masquer sa véritable identité
4. ne pas tenter de lire, modifier, copier ou détruire des ressources informatiques autres que celles auxquelles l'employeur lui a donné accès
5. ne pas proposer ou rendre accessible aux tiers des données et informations confidentielles, protégées ou non,
6. utiliser les ressources informatiques conformément à la législation en vigueur
7. ne pas introduire de virus dans le système informatique, notamment par le biais de sources douteuses (ouverture d'attachements à des courriers provenant d'inconnus, téléchargement de fichiers issus de sites douteux ou non sécurisés par exemple pas en https)
8. ne pas connecter de périphérique de stockage de masse (clé USB, disque dur externe, carte SD, etc.) sans l'autorisation expresse de l'employeur
9. ne pas installer lui-même aucun logiciel même freeware sur son poste
10. ne pas modifier pas la configuration de son poste ni des applications qu'il utilise
11. respecter scrupuleusement la règlementation sur la protection des données personnelles
12. ne pas procéder à des copies sur tous types de média informatiques en infraction avec les droits de propriété intellectuelle
13. ne pas télécharger ou installer des logiciels ou tout autre contenu soumis à des droits d'auteur sans autorisation expresse de l'employeur
14. ne pas se connecter ni transférer en interne ou vers l'extérieur des contenus illégaux ou contraire aux bonnes mœurs

De plus, si le collaborateur dispose d'un outil mobile appartenant à l'employeur ou s'il bénéficie, moyennant accord express de l'employeur, d'un accès aux ressources informatiques avec ses propres outils connectés, il veillera également :

1. à ne jamais laisser seul le PC portable ou l'équipement mobile dans une voiture ou dans un endroit où il serait facilement accessible à des personnes mal intentionnées
2. en cas de perte ou de vol, à avertir immédiatement l'employeur qui bloquera immédiatement les accès aux ressources informatiques
3. à respecter pour ces outils connectés les règles de sécurité énoncées dans la présente charte

Les infractions au contenu de cette charte feront, en fonction de leur gravité, soit l'objet de sanctions telles que celles prévues dans le règlement de travail, soit l'objet de poursuites, pénales ou civiles, suivant la gravité de l'infraction constatée.

Je soussigné, .NGUYEN....Celine....., reconnais avoir reçu un exemplaire de la présente, en avoir pris connaissance.

Fait en double exemplaire à Woluwé-Saint-Lambert, le .22/09/2020

Signature de l'employeur

VINAIMONT André

Signature du collaborateur

Annexe 5 – Cécile

Le (la) soussigné(e) Cécile Poulain

autorise

MYASSURANCE.BE SPRL
Avenue des Touristes 7 – 1150 Woluwé-Saint-Pierre
0671919394
Représenté par Nicolas Rubbers et Audrine Vinaimont

à utiliser, reproduire et communiquer les images fixes et/ou séquences vidéo (ci-après les « Images ») décrites dans l'annexe ci-jointe (qui fait partie intégrante de la présente autorisation), en tout ou en partie, intégrées ou non avec d'autres images fixes ou animées, modifiées, retouchées ou non, en édition sur tout support papier, textile, plastique, ou autres, en diffusion sur tout support vidéo digital ou non, et en intégration sur tout support électronique y compris l'internet et l'intranet, et ce, sans limitation de durée à compter de la signature de la présente.

Cette autorisation est accordée pour toute zone de diffusion tant en Belgique qu'à l'étranger : (cocher la ou les cases appropriées ci-dessous) :

O pour toute communication interne et externe à MYASSURANCE.BE SPRL, et notamment la presse interne d'entreprise, toute plaquette institutionnelle ou rapport annuel, et donc à l'exclusion de toute utilisation commerciale ou publicitaire, c'est-à-dire donnant lieu à de l'achat d'espace publicitaire dans tous supports externes

O pour toute utilisation publicitaire (donnant lieu à de l'achat d'espace publicitaire dans tous supports externes ou sur tous supports publicitaires ou commerciaux, packaging, édition, presse, design, marketing direct, etc.) réalisée par ou pour MYASSURANCE.BE SPRL.

Cette autorisation est valable pour une période de 5 ans à compter de la date de signature de la présente et pourra être prolongée.

MYASSURANCE.BE SPRL s'engage à respecter la réglementation concernant le droit au respect des données personnelles dans le cadre des finalités de cette autorisation conformément à la politique de vie privée jointe en annexe 2.

Le (la) soussigné(e) renonce expressément à toute rétribution de quelque nature que ce soit concernant l'utilisation des Images pour les usages prévus dans la présente autorisation.

Le (la) soussigné(e) certifie disposer pleinement des droits cédés, comprends et accepte que la présente autorisation n'oblige nullement MYASSURANCE.BE SPRL à utiliser les Images. Un retrait de la présente autorisation ne pourra être obtenu que moyennant l'envoi par le soussigné d'un courrier recommandé adressé à MYASSURANCE.BE SPRL. Le retrait de l'autorisation ne sera effectif, en tout état de cause, qu'au plus tôt 6 mois après la réception du courrier et ce retrait ne concernera pas les utilisations des images sur des supports existants ou en voie de réalisation à la date de la réception du courrier et ce, pour toute la durée de vie de ces supports.

Fait à Ottignies le 22/09/2020 en deux exemplaires,

Nom : Poulain Cécile

Signature :

VINAIMONT
AUDRINE

ANNEXE 1: DESCRIPTION DES IMAGES FAISANT L'OBJET DE LA PRESENTE CESSION

Photo d'équipe et photo personnelle effectuée dans le cadre de l'agence et spécifiquement pour MyAssurance.be

ANNEXE 2

Politique de respect des Données à caractère personnel pour les images faisant l'objet de la présente cession de droit à l'image

Responsable de traitement : MYASSURANCE.BE SPRL dont les coordonnées sont indiquées ci-dessus, et ci-après appelé « Nous »

Nous nous engageons à respecter la vie privée des personnes rencontrées dans le cadre de nos activités. Les images faisant l'objet de la présente cession étant des données personnelles, cette politique de vie privée s'applique à ces images (ci-après les Images)

Cette Politique de respect des Données à caractère personnel (ci-après la Politique) décrit la manière dont nous gérons les Images en tant que données à caractère personnel. Nous traitons vos données à caractère personnel en conformité avec toutes les règlementations applicables concernant la protection des données personnelles.

En acceptant la présente Politique, vous reconnaissez et acceptez les termes de la Politique ainsi que les traitements et les transferts de Données à caractère personnel qui seront réalisés conformément à la Politique.

Les Données à caractère personnel que nous collectons dans le cadre de nos relations, sont

- Informations personnelles : nom, adresse, e-mail, numéros de téléphone, numéro de gsm, sexe, état civil

- Informations financières : numéro de compte bancaire en cas de rémunération

Les données que nous recueillons proviennent :

- De votre inscription auprès de nous en signant le présent document
- Des Images

Nous utilisons ces Données à caractère personnel pour :

- Répondre à vos demandes et communiquer avec vous et d'autres dans le cadre de nos activités.
- Vous permettre d'accéder aux informations que nous mettons en ligne à disposition des utilisateurs de nos services
- les usages prévus ci-dessus dans la présente cession de droits
- Résoudre les réclamations
- Gérer les droits d'accès, de rectification, d'effacement,… prévus par la législation
- Se conformer aux lois et obligations réglementaires applicables

Les bases légales de traitement sont les suivantes :

- votre consentement par la signature de la présente (nous vous rappelons qu'à tout moment vous avez le droit de retirer votre consentement) ;
- le traitement est nécessaire à l'exécution du présent contrat ;

Si nous étions amenés à traiter les Données à caractère personnel pour d'autres finalités que celles proposées ci-dessus nous ne le ferions que dans le cadre des bases légales précisées ci-dessus.

Nous n'utilisons pas de techniques de prise de décision fondée sur un traitement automatisé produisant des effets juridiques concernant la personne concernée ou l'affectant de manière significative.

Les Images pourront être accessibles aux organisations suivantes :

- les autorités gouvernementales ou publiques en fonction des lois applicables
- nos sous-traitants, notamment nos fournisseurs informatiques, dans le cadre contractuel prévu par la règlementation sur la protection des données personnelles
- nos partenaires, vendeurs, agences de marketing dans le cadre de nos activités commerciales
- des tiers dans le cadre de réorganisation interne, de cession de fonds de commerce, de fusion ou acquisition

Nous ne transférons pas de données en dehors de l'Union Européenne

Nous prenons les mesures techniques et organisationnelles appropriées qui sont en conformité avec la règlementation en matière de vie privée et de protection des données applicables. Nous avons signé avec nos sous-traitants des contrats par lesquels ils nous

garantissent d'avoir pris les mesures de sécurité techniques et organisationnelles appropriées.

Vos données sont effacées après les durées suivantes : (conseil de GDPRFOLDER.EU, nous recommandons de détruire les images 5 ans après la prise de vue)

- 5 ans après la prise des photos
- En vertu des obligations légales de conservation, ou d'une décision du responsable de traitement pour ce qui concerne les supports sur lesquels les Ipmages ont été utilisées comme précisé dans la cession de droit ci-dessus

Vous avez le droit d'accéder à vos données, de les rectifier en cas de besoin, de vous opposer à leur utilisation, de demander leur effacement, leur limitation ou leur portabilité. Si vous souhaitez utiliser un de ces droits, veuillez nous contacter à notre adresse de contact en prouvant votre identité au moyen d'une copie de votre carte d'identité.

Vous avez également le droit de porter plainte auprès de l'autorité de protection des données

Nous revoyons les règles contenues dans la présente Politique régulièrement et nous nous réservons le droit d'apporter des changements à tout moment afin de prendre en compte des changements dans nos activités et des exigences légales.

Nous vous invitons à consulter régulièrement notre site internet, la date de mise à jour sera indiquée. En cas de changement important nous nous permettrons de reprendre contact avec vous pour vous signaler ces changements.

Annexe 5 - Céline

Le (la) soussigné(e) ...NGUYEN Céline

autorise

MYASSURANCE.BE SPRL
Avenue des Touristes 7 – 1150 Woluwé-Saint-Pierre
0671919394
Représenté par Nicolas Rubbers et Audrine Vinaimont

à utiliser, reproduire et communiquer les images fixes et/ou séquences vidéo (ci-après les « Images ») décrites dans l'annexe ci-jointe (qui fait partie intégrante de la présente autorisation), en tout ou en partie, intégrées ou non avec d'autres images fixes ou animées, modifiées, retouchées ou non, en édition sur tout support papier, textile, plastique, ou autres, en diffusion sur tout support vidéo digital ou non, et en intégration sur tout support électronique y compris l'internet et l'intranet, et ce, sans limitation de durée à compter de la signature de la présente.

Cette autorisation est accordée pour toute zone de diffusion tant en Belgique qu'à l'étranger : (cocher la ou les cases appropriées ci-dessous) :

O pour toute communication interne et externe à MYASSURANCE.BE SPRL, et notamment la presse interne d'entreprise, toute plaquette institutionnelle ou rapport annuel, et donc à l'exclusion de toute utilisation commerciale ou publicitaire, c'est-à-dire donnant lieu à de l'achat d'espace publicitaire dans tous supports externes

O pour toute utilisation publicitaire (donnant lieu à de l'achat d'espace publicitaire dans tous supports externes ou sur tous supports publicitaires ou commerciaux, packaging, édition, presse, design, marketing direct, etc.) réalisée par ou pour MYASSURANCE.BE SPRL.

Cette autorisation est valable pour une période de 5 ans à compter de la date de signature de la présente et pourra être prolongée.

MYASSURANCE.BE SPRL s'engage à respecter la réglementation concernant le droit au respect des données personnelles dans le cadre des finalités de cette autorisation conformément à la politique de vie privée jointe en annexe 2.

Le (la) soussigné(e) renonce expressément à toute rétribution de quelque nature que ce soit concernant l'utilisation des Images pour les usages prévus dans la présente autorisation.

Le (la) soussigné(e) certifie disposer pleinement des droits cédés, comprends et accepte que la présente autorisation n'oblige nullement MYASSURANCE.BE SPRL à utiliser les Images. Un retrait de la présente autorisation ne pourra être obtenu que moyennant l'envoi par le soussigné d'un courrier recommandé adressé à MYASSURANCE.BE SPRL. Le retrait de l'autorisation ne sera effectif, en tout état de cause, qu'au plus tôt 6 mois après la réception du courrier et ce retrait ne concernera pas les utilisations des images sur des supports existants ou en voie de réalisation à la date de la réception du courrier et ce, pour toute la durée de vie de ces supports.

Fait à Ottignies le ..22/09/2020.. en deux exemplaires,

Nom : ..NGUYEN..... Signature : .....

DINANTONI

ANNEXE 1: DESCRIPTION DES IMAGES FAISANT L'OBJET DE LA PRESENTE CESSION

Photo d'équipe et photo personnelle effectuée dans le cadre de l'agence et spécifiquement pour MyAssurance.be

ANNEXE 2

Politique de respect des Données à caractère personnel pour les images faisant l'objet de la présente cession de droit à l'image

Responsable de traitement : MYASSURANCE.BE SPRL dont les coordonnées sont indiquées ci-dessus, et ci-après appelé « Nous »

Nous nous engageons à respecter la vie privée des personnes rencontrées dans le cadre de nos activités. Les images faisant l'objet de la présente cession étant des données personnelles, cette politique de vie privée s'applique à ces images (ci-après les Images)

Cette Politique de respect des Données à caractère personnel (ci-après la Politique) décrit la manière dont nous gérons les Images en tant que données à caractère personnel. Nous traitons vos données à caractère personnel en conformité avec toutes les règlementations applicables concernant la protection des données personnelles.

En acceptant la présente Politique, vous reconnaissez et acceptez les termes de la Politique ainsi que les traitements et les transferts de Données à caractère personnel qui seront réalisés conformément à la Politique.

Les Données à caractère personnel que nous collectons dans le cadre de nos relations, sont

- Informations personnelles : nom, adresse, e-mail, numéros de téléphone, numéro de gsm, sexe, état civil

- Informations financières : numéro de compte bancaire en cas de rémunération

Les données que nous recueillons proviennent :

- De votre inscription auprès de nous en signant le présent document
- Des Images

Nous utilisons ces Données à caractère personnel pour :

- Répondre à vos demandes et communiquer avec vous et d'autres dans le cadre de nos activités.
- Vous permettre d'accéder aux informations que nous mettons en ligne à disposition des utilisateurs de nos services
- les usages prévus ci-dessus dans la présente cession de droits
- Résoudre les réclamations
- Gérer les droits d'accès, de rectification, d'effacement,… prévus par la législation
- Se conformer aux lois et obligations réglementaires applicables

Les bases légales de traitement sont les suivantes :

- votre consentement par la signature de la présente (nous vous rappelons qu'à tout moment vous avez le droit de retirer votre consentement) ;
- le traitement est nécessaire à l'exécution du présent contrat ;

Si nous étions amenés à traiter les Données à caractère personnel pour d'autres finalités que celles proposées ci-dessus nous ne le ferions que dans le cadre des bases légales précisées ci-dessus.

Nous n'utilisons pas de techniques de prise de décision fondée sur un traitement automatisé produisant des effets juridiques concernant la personne concernée ou l'affectant de manière significative.

Les Images pourront être accessibles aux organisations suivantes :

- les autorités gouvernementales ou publiques en fonction des lois applicables
- nos sous-traitants, notamment nos fournisseurs informatiques, dans le cadre contractuel prévu par la règlementation sur la protection des données personnelles
- nos partenaires, vendeurs, agences de marketing dans le cadre de nos activités commerciales
- des tiers dans le cadre de réorganisation interne, de cession de fonds de commerce, de fusion ou acquisition

Nous ne transférons pas de données en dehors de l'Union Européenne

Nous prenons les mesures techniques et organisationnelles appropriées qui sont en conformité avec la règlementation en matière de vie privée et de protection des données applicables. Nous avons signé avec nos sous-traitants des contrats par lesquels ils nous

garantissent d'avoir pris les mesures de sécurité techniques et organisationnelles appropriées.

Vos données sont effacées après les durées suivantes : (conseil de GDPRFOLDER.EU, nous recommandons de détruire les images 5 ans après la prise de vue)

- 5 ans après la prise des photos
- En vertu des obligations légales de conservation, ou d'une décision du responsable de traitement pour ce qui concerne les supports sur lesquels les Ipmages ont été utilisées comme précisé dans la cession de droit ci-dessus

Vous avez le droit d'accéder à vos données, de les rectifier en cas de besoin, de vous opposer à leur utilisation, de demander leur effacement, leur limitation ou leur portabilité. Si vous souhaitez utiliser un de ces droits, veuillez nous contacter à notre adresse de contact en prouvant votre identité au moyen d'une copie de votre carte d'identité.

Vous avez également le droit de porter plainte auprès de l'autorité de protection des données

Nous revoyons les règles contenues dans la présente Politique régulièrement et nous nous réservons le droit d'apporter des changements à tout moment afin de prendre en compte des changements dans nos activités et des exigences légales.

Nous vous invitons à consulter régulièrement notre site internet, la date de mise à jour sera indiquée. En cas de changement important nous nous permettrons de reprendre contact avec vous pour vous signaler ces changements.