

POLITIQUE DE PROTECTION DE LA VIE PRIVEE

OPTINITI – 26/12/2023

1. INTRODUCTION

La politique de protection de la vie privée défini et informe les visiteurs, clients (potentiels et actuels) et employés de clients, ci-après "le Sujet des Données", de la manière dont OPTINITI SRL (ci-après "nous", "Optiniti" ou "la Société"), utilise et protège les informations qui lui sont fournies et, en particulier mais pas exclusivement, lorsque les " le Sujet des Données " utilisent le site internet d'Optiniti, accessible via le lien suivant : <https://www.optiniti-group.com/>; ci-après "le Site Web", ou lorsque les " le Sujet des Données " font appel à ou utilisent un des services proposés par Optiniti.

Nous n'accédons ni n'utilisons vos données personnelles pour une autre objectif que de fournir, maintenir et améliorer nos services et dans les cas où la loi l'exige. Nous obtenons et détenons les informations personnelles de manière à pouvoir gérer les différents plans d'incentive destinés aux employés de nos clients.

Cette politique défini la manière dont nous gérons ces informations de manière à veiller à ce que nous respectons nos obligations en matière de respect de la vie privée de nos clients et de manière à ce que ces informations restent confidentielles. Ces obligations contraignantes découlent du cadre légal et réglementaire régissant le traitement et la protection des données personnelles en Belgique et en particulier le Règlement Général sur la Protection des Données (le "RGPD") (EU) 2016/679 et la loi de 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (la "Loi") qui a été adoptée pour la mise en œuvre effective de certaines dispositions du RGPD.

2. QUI SOMMES NOUS ?

Optiniti, une société de droit belge ayant ses bureaux enregistrés Avenue Commandant Lachouque 33, 1410 Waterloo (TVA BE0792213945) est le responsable du traitement des données (qui est chargé de déterminer la finalité et les modalités d'utilisation de vos données à caractère personnel).

Optiniti SRL

Email: support@optiniti-group.com

Le responsable du traitement des données doit s'assurer de la justesse et de l'utilité des données personnelle collectées et traitées. Outre ce qui précède, il veille à respecter les réglementations applicables et la présente politique de protection de la vie privée.

Nous nous engageons à faire ce qu'il faut lorsqu'il s'agit de la manière de collecter, utiliser et protéger vos données personnelles et c'est pour cette raison que Nous avons élaboré cette politique de protection de la vie privée (la "Politique"), qui :

- Décrit les différentes manières d'interagir avec Nous et le type de données personnelles que nous collectons ;
- Explique les raisons pour lesquelles Nous utilisons les données que nous collectons ;
- Explique quand et pourquoi Nous partagerons vos données au sein d'Optiniti et avec d'autres organisations (décrites ci-dessous) ; and
- Explique les droits et choix que dont vous disposez en matière de données personnelles.

3. QUE VOULONS NOUS DIRE PAR DONNEES PERSONNELLES ?

Les données personnelles sont toutes les informations relatives à vous ainsi que les données qui pourraient servir à vous identifier directement ou indirectement.

De manière Générale, il est possible de visiter le Site Web sans fournir de données personnelles. Dans tous les cas, le Sujet des Données n'est d'aucune manière obliger de transmettre ses informations à le Société.

Cependant, dans certaines situations, si les informations ne sont pas fournies, il est possible que le Sujet des Données ne soient pas capable de bénéficier des services requis. En effet, de manière à ce que le Sujet des Données puissent bénéficier des services offerts par la Société, Optiniti pourrait être amener à, dans certains cas, devoir demander au Sujet des Données ou à son employeur de fournir nom(s) de famille, prénom(a), genre, langue, nationalité, adresse, numéro de registre national, numéro de téléphone, adresse email, ci-après appelés les "Informations Personnelles". En fournissant ces Informations Personnelles, le Sujet des Données accepte expressément son traitement par Optiniti aux fins indiquées au point 6 ci-dessous ainsi qu'aux fins indiquées lors de chaque demande.

Conformément au RGPD du 14 avril 2016, le Société vous informe qu'Optiniti pourrait vous demander d'autres documents qui pourraient être nécessaires à la gestion effective des plans d'incentive dont vous feriez partie.

4. DE QUELLE SORTE D'INFORMATIONS AVONS NOUS BESOIN ET POURQUOI ?

Lorsque vous accédez à notre Site Web ou à notre plateforme via le Site Web, Nous pouvons collecter vos Informations Personnelles à partir de votre navigation sur le Site Web et de vos connections à la Plateforme.

Nous traitons les Informations Personnelles que nous recevons de votre part dans le cadre de la relation contractuelle liant Optiniti avec votre employeur ou aux fins des intérêts légitimes poursuivis par Optiniti. Nous pouvons également traiter des données que nous avons reçu de manière légitime de sources et bases de données d'identification publiques. En principe, nous sommes obligés ou avons besoin de détenir vos données pour plusieurs raisons :

- Dans le cadre de l'établissement et du maintien d'une relation contractuelles, nous sommes tenus de collecter vos Informations Personnelles afin de nous permettre d'établir et de vérifier votre identité. Pour ce faire, Nous vous demanderons des données personnelles qui comprennent, sans s'y limiter, votre nom complet, votre pays de résidence, votre adresse, votre date de naissance, votre nationalité, votre numéro de registre national, votre adresse email ou d'autres informations de contact ;
- Afin de faciliter vos transactions, Nous pouvons traiter vos coordonnées IBAN et d'autres informations relatives au traitement des paiements, comme le demandent les fournisseurs de service de paiement ;
- Pour évaluer l'adéquation de nos services à votre situation et à votre expérience, Nous pouvons vous demander des informations supplémentaires telles que, mais sans s'y limiter, l'expérience lors de l'utilisation du logiciel, les détails de l'emploi, les connaissances, expérience en matière de services et de produits financiers ;

Nous pouvons également collecter ou être enjoint à collecter et traiter des informations à votre sujet via votre utilisation de notre plateforme. Ces informations peuvent inclure, entre autres :

- L'adresse Internet Protocol (IP) utilisée pour connecter votre ordinateur au réseau internet, vos informations de connexion, votre localisation géographique, votre navigateur et le type et la version du plug-in du navigateur, votre système d'exploitation et votre plateforme ainsi que d'autres données personnelles indirectes. Lorsque Nous traitons de telles informations, Nous nous efforçons de toujours les utiliser de manière agrégée et anonyme ;
- Toute autre donnée personnelle qui peut être nécessaire afin de se conformer aux règles en vigueur ; and
- Toute autre donnée personnelle qui peut être nécessaire afin de régler un litige ou préparer une défense juridique.

5. COMMENT SONT COLLECTEES VOS DONNEES PERSONNELLES ?

Nous collectons la plupart de ces données personnelles directement auprès de votre employeur, par le biais de notre logiciel/plateforme sécurisé(e) qui permet le partage de fichiers. Cependant, dans certains cas :

Nous pouvons vous demander, à vous ou à votre employeur, des informations supplémentaires par courrier électronique ou par le biais de notre formulaire de contact, et nous pouvons également utiliser nos propres dossiers et des informations provenant d'autres sources pour nous conformer à nos obligations légales et réglementaires.

Le traitement et le stockage de vos données personnelles sont nécessaires pour fournir les services convenus avec votre employeur et décrits dans l'accord de collaboration entre Optiniti et votre employeur, ainsi que pour nous conformer à nos obligations réglementaires. Si vous choisissez de ne pas nous fournir certaines des informations demandées, il se peut que nous ne soyons pas en mesure de vous intégrer en tant que nouveau bénéficiaire d'un plan d'intéressement ou de mettre fin aux services fournis dans le cadre d'un plan existant.

Nous maintenons les informations à jour autant que possible et nous modifions rapidement tout détail, tel que votre adresse, lorsque vous nous informez de leur changement.

Les données personnelles susceptibles d'être traitées par Optiniti comprennent tout type de communications électroniques telles que lettres, courriels, conversations téléphoniques, numéro d'identification fiscale et toute information fiscale associée, toute information personnelle résultant des contrôles "Know Your Customer" et "Anti Money Laundering" effectués par Optiniti conformément à la législation applicable en matière de lutte contre le blanchiment d'argent et le financement du terrorisme.

Votre utilisation de la plate-forme implique la collecte automatisée de certains types d'informations, dont certaines peuvent être considérées comme des informations personnelles. Ces informations comprennent : l'adresse IP, le type de navigateur et le système d'exploitation.

En outre, le site web utilise une série de cookies pour améliorer et personnaliser votre expérience. Vous trouverez de plus amples informations à ce sujet dans notre politique en matière de cookies.

6. POURQUOI AVONS-NOUS BESOIN DE CES INFORMATIONS ET SUR QUELLE BASE JURIDIQUE LES DONNEES SONT-ELLES TRAITEES ?

Légitimité du traitement des données

Nous traiterons vos données à caractère personnel (y compris la collecte, l'utilisation, le stockage et le transfert, le cas échéant) :

- pour la gestion efficace des plans de participation décrits dans l'accord de collaboration conclu entre votre employeur en tant que client et Optiniti (les " services ") ;
- pour le respect des obligations légales et réglementaires auxquelles Optiniti est soumis (y compris, mais sans s'y limiter, les obligations découlant de la réglementation MIFID 2, les obligations réglementaires en matière de lutte contre le blanchiment d'argent et le financement du terrorisme, toute législation fiscale applicable, etc.), EMIR, etc.), EMIR, etc. Ces obligations réglementaires comprennent notamment : les obligations de déclaration aux autorités EMIR ; la fourniture d'informations aux autorités chargées de la lutte contre la criminalité financière en cas de transactions suspectes de blanchiment d'argent ou dans le cadre de procédures pénales financières ; la fourniture d'informations aux autorités fiscales. Veuillez noter que pour répondre à certaines des exigences susmentionnées, nous pouvons avoir recours à la prise de décision automatisée et au profilage, bien que vous puissiez demander une intervention humaine, mais vous ne pourrez pas vous opposer à un tel traitement.
- Dans le cas où le traitement des données personnelles est nécessaire aux fins des intérêts légitimes poursuivis par Optiniti - par exemple, si cela est nécessaire - pour nous assurer que nous vous fournissons les meilleurs services et informations possibles et pour continuer à améliorer nos produits dans votre intérêt.
- Dans le cadre de votre consentement - par exemple, à des fins de marketing et de promotion. Si vous nous avez donné votre accord pour traiter vos données à caractère personnel à des fins de marketing, le traitement n'aura lieu que conformément aux objectifs énoncés dans la déclaration de consentement et dans la mesure convenue dans cette déclaration. Tout consentement donné peut être révoqué à tout moment par vous avec effet futur.

Objectifs

Optiniti traitera et analysera vos données personnelles directes (telles que votre nom, votre date de naissance, votre ID, etc.) et indirectes (telles que les données d'analyse et de suivi) en combinaison avec l'utilisation de votre compte dans le but de :

- fournir les services demandés par votre employeur et fournis dans le cadre de l'accord de collaboration, y compris, entre autres, la vérification ;
 - o la vérification de votre identité, l'ouverture et la gestion de votre compte sur la Plateforme;
 - o répondre à nos obligations réglementaires;
 - o traiter vos demandes relatives aux services;
 - o gérer les relations avec les clients par le biais de communications électroniques, téléphoniques ou par chat, conclure et exécuter des transactions portant sur des instruments financiers;
 - o effectuer un contrôle de la gestion des risques, une analyse des données et une supervision globale de vos besoins permanents et améliorer les services qui vous sont offerts;
 - o l'amélioration et la personnalisation de nos services afin d'améliorer votre expérience;
 - o la prévention des abus et des fraudes, la démonstration des transactions commerciales et des communications, la gestion de la surveillance des transactions, le contrôle et le respect des obligations de déclaration, la gestion des risques, des différends, des plaintes, des litiges ou dans le cadre de poursuites judiciaires.;
- envoi de la lettre d'information électronique à la personne concernée;
- fournir les informations ou services demandés par la personne concernée (par présence sur les sites d'exploitation, par e-mail, par téléphone ou par courrier) et adaptés à la personne concernée, et plus particulièrement :
 - o le traitement et le suivi des demandes de prix et/ou d'informations adressées à l'entreprise;
 - o la présentation des services offerts et fournis par l'entreprise;
 - o des statistiques sur les visites du site web de l'entreprise;
 - o collecter des informations permettant à la société d'améliorer le site Web, les produits et les services (notamment par le biais de cookies);
 - o à Google Analytics, au moyen de cookies, comme indiqué ci-dessous et/ou dans la clause de non-responsabilité qui peut être consultée sur le site web de l'entreprise via le lien suivant :<https://optiniti-group.odoo.com/cookie-policy>

7. QUI SONT LES DESTINATAIRES DE VOS DONNEES PERSONNELLES?

Vos données personnelles sont reçues et traitées par les employés d'Optiniti qui en ont besoin pour l'exécution des obligations contractuelles, légales et réglementaires. En outre, nous pouvons divulguer, dans la mesure où nous estimons qu'une telle divulgation ou transmission est nécessaire pour atteindre les objectifs énoncés ci-dessus, aux destinataires suivants:

- D'autres sociétés partenaires d'Optiniti, telles que le(s) fournisseur(s) de logiciels. Ces données peuvent être transférées afin de nous permettre de vous fournir un service complet, lorsque d'autres sociétés effectuent des composants de l'offre de service complet tels que la maintenance informatique ou les services d'assistance;
- Tout avocat, auditeur ou conseiller externe, consultant professionnel, agence de référence de crédit, notaire, huissier de justice, ainsi que tout tribunal, organisme réglementaire, gouvernemental, administratif ou autre organisme officiel, comme convenu ou pouvant être requis par la loi, lorsque cette divulgation est nécessaire.
 - (i) se conformer à toute loi ou réglementation applicable;
 - (ii) pour faire appliquer les conditions générales ou les politiques en vigueur;
 - (iii) protéger la sécurité ou l'intégrité de nos services ; et
 - (iv) pour protéger nos droits et nos intérêts;
- Les prestataires de services tiers ou les processeurs de données qui fournissent des services informatiques, des vérifications d'identité, des services bancaires et de traitement des paiements ou d'autres services à Optiniti, qui sont uniquement autorisés à traiter vos données personnelles dans le strict but de fournir ces services et conformément à nos instructions. Le cas échéant, nous concluons avec ces prestataires de services tiers les accords contractuels pertinents ou les clauses standard de protection des données qui seraient exigés en vertu des lois de protection des données pertinentes pour assurer la conformité avec nos instructions ; et
- des tiers dans le cadre de fusions et d'acquisitions, à condition que l'acheteur ou le vendeur potentiel s'engage à respecter vos données à caractère personnel d'une manière conforme à notre politique de protection de la vie privée.

Nous demanderons à toute entité à laquelle nous divulguons vos informations ou qui peut les obtenir en notre nom de garantir leur confidentialité et de les traiter conformément à l'objectif légitime pour lequel elle est autorisée à y accéder et conformément aux lois applicables en matière de protection des données.

Nous ne partagerons ni ne vendrons vos informations à des tiers à des fins commerciales ou de marketing sans votre consentement.

Transfert d'informations au niveau international

Les données à caractère personnel peuvent être conservées dans nos bureaux et au sein d'agences, de prestataires de services, de représentants, d'auditeurs, d'avocats et d'agents tiers, comme décrit ci-dessus. Certains de ces tiers peuvent être basés en dehors de l'UE et de l'Espace économique européen (EEE).

En vertu de la législation sur la protection des données, nous ne pouvons transférer vos données à caractère personnel vers un pays ou une organisation internationale en dehors de l'UE/EEE que dans les cas suivants :

- la Commission européenne a décidé que le pays ou l'organisation internationale en question assure un niveau de protection adéquat des données à caractère personnel (décision dite "d'adéquation");
- il existe des garanties appropriées, ainsi que des droits exécutoires et des voies de recours efficaces pour les personnes concernées ; ou
- une exception spécifique s'applique en vertu de la loi sur la protection des données.

Décision de conformité

Nous pouvons transférer vos données à caractère personnel vers certains pays, sur la base d'une décision de conformité. La liste des pays bénéficiant de décisions d'adéquation changera de temps à autre. Nous chercherons toujours à nous appuyer sur une décision d'adéquation, lorsqu'elle existe.

Les autres pays vers lesquels nous sommes susceptibles de transférer des données à caractère personnel ne bénéficient pas d'une décision d'adéquation. Cela ne signifie pas nécessairement qu'ils offrent une mauvaise protection des données à caractère personnel, mais nous devons envisager d'autres motifs pour transférer les données à caractère personnel, par exemple en veillant à ce que des garanties appropriées soient en place ou en nous appuyant sur une exception, comme expliqué ci-dessous.

Elles peuvent être traitées par du personnel travaillant pour nous ou pour l'un de nos fournisseurs, situé en dehors de l'UE et/ou de l'EEE. Ce personnel peut, par exemple, être impliqué dans l'exécution de nos services d'assistance. Nous prendrons toutes les mesures nécessaires pour garantir que vos données à caractère personnel sont traitées en toute sécurité et conformément à la présente politique de confidentialité et nous avons adopté des mesures de sauvegarde appropriées pour les protéger.

Transfert avec ces garanties appropriées

En l'absence de décision de conformité, nous pouvons transférer vos données à caractère personnel vers un autre pays si nous sommes convaincus que le transfert est conforme à la législation sur la protection des données, que des garanties appropriées sont en place et que vous disposez, en tant que personne concernée, de droits exécutoires et de voies de recours efficaces.

Les garanties comprennent généralement l'utilisation de clauses contractuelles standard de protection des données approuvées par la loi. De cette manière, nous concluons des accords contraignants avec ces tiers afin que vos informations soient protégées selon les mêmes normes que dans l'UE et l'EEE.

8. COMBIEN DE TEMPS VOS DONNÉES SERONT-ELLES CONSERVÉES ?

Nous traiterons vos données à caractère personnel pendant toute la durée de l'accord de collaboration que votre employeur a conclu avec nous et pendant une période de dix (10) ans après la résiliation de l'accord afin de nous conformer à la législation applicable en matière de lutte contre le blanchiment d'argent et aux obligations légales de conservation. En outre, les données à caractère personnel ne seront pas conservées plus longtemps que le temps nécessaire à la réalisation des objectifs de leur traitement, sous réserve des délais de prescription légaux généraux et de la période de conservation mentionnée lorsque les lois applicables exigent que les données à caractère personnel soient conservées pendant une certaine période après la fin de notre relation commerciale avec vous.

9. QUELS SONT VOS DROITS CONCERNANT LE TRAITEMENT DE VOS DONNÉES PERSONNELLES ?

Vous avez le droit de:

Droits d'accès et communication des données

La personne concernée a le droit d'accéder aux données personnelles que la société détient à son sujet et de les consulter. La personne concernée peut également savoir comment l'entreprise a obtenu les données et à qui elles ont été communiquées. La personne concernée peut également demander une copie de ces données personnelles en cours de traitement.

En raison de l'obligation de sécurité et de confidentialité qui incombe à la société dans le cadre du traitement des données à caractère personnel, la demande d'accès et de consultation des données par la personne concernée sera traitée sous réserve de la justification de son identité, notamment par la production d'une copie électronique ou papier (accompagnée d'une signature) de sa carte d'identité pendant la durée de validité de celle-ci. La demande est, en tout état de cause, gratuite pour la personne concernée.

Toutefois, l'entreprise peut s'opposer aux demandes manifestement abusives ou infondées (par leur nombre ou leur caractère répétitif ou systématique, par exemple).

Droit de rectification des données

Le règlement européen permet à la personne concernée de demander la rectification, la mise à jour ou la suppression des données la concernant qui peuvent être inexactes, erronées, incomplètes ou obsolètes.

Droit d'opposition

La personne concernée a le droit de s'opposer au traitement des données dans les deux situations suivantes :

- lorsque l'exercice de ce droit est fondé sur des motifs légitimes ou
- lorsque l'exercice de ce droit vise à empêcher que les données collectées soient utilisées à des fins de prospection commerciale.

Droit de restriction

La personne concernée peut demander à l'entreprise de limiter le traitement de ses données personnelles dans certaines circonstances, par exemple lorsqu'elle conteste l'exactitude des informations personnelles, pendant un certain temps pour permettre à Optiniti de vérifier l'exactitude de ses données personnelles ou dans le cas où elle estime que le traitement est illégal. Cependant, une telle objection ne peut pas nous empêcher de stocker ses informations personnelles.

Droit à l'effacement

La personne concernée a le droit de demander et d'obtenir la suppression des données la concernant détenues par la société.

L'entreprise répondra à la demande de la personne concernée si :

- données à caractère personnel ne sont plus nécessaires aux fins pour lesquelles elles ont été collectées ;
- le traitement des données était fondé exclusivement sur le consentement de la personne concernée et celle-ci retire son consentement ;
- la personne concernée s'oppose au traitement pour des raisons fondées.

En tout état de cause, la demande d'effacement peut être refusée par l'entreprise si elle est nécessaire à l'exercice ou à la défense de droits en justice ou au respect d'une obligation légale ou contractuelle de l'entreprise.

Droit à la portabilité des données

La personne concernée peut demander que ses données à caractère personnel soient transférées à un responsable du traitement identique à l'entreprise. La personne concernée peut donc demander que les données soient transmises à l'entreprise dans un format structuré, couramment utilisé et lisible par ordinateur.

Comment exercer vos droits

Les droits susmentionnés peuvent être exercés en envoyant une lettre à l'adresse de l'entreprise ou en envoyant un courrier électronique à l'adresse suivante : support@optiniti-group.com.

Temps de réponse

L'entreprise répondra à la demande de la personne concernée de la même manière que la personne concernée a exercé son droit.

L'entreprise s'engage à répondre à toute demande d'accès, de rectification ou d'opposition, de suppression ou à toute autre demande complémentaire d'information dans un délai raisonnable et en tout état de cause dans un délai maximum de 1 mois à compter de la réception de votre demande.

En fonction de la complexité de la demande, le délai de réponse peut être étendu à 3 mois, conformément au règlement européen applicable.

19. COMMENT GERONS-NOUS ET PROTEGEONS-NOUS VOS DONNEES PERSONNELLES?

Nous déployons beaucoup d'efforts et appliquons les normes techniques et organisationnelles les plus élevées pour garantir la sécurité et la confidentialité de vos données à caractère personnel. Toutes les données à caractère personnel que vous nous fournissez sont stockées sur des serveurs sécurisés et nous appliquons des procédures rigoureuses pour les protéger contre la perte, l'utilisation abusive, l'accès non autorisé, l'altération, la divulgation ou la destruction de vos données à caractère personnel. Nous protégeons vos informations personnelles en appliquant des mesures de protection physiques, électroniques et procédurales conformément aux lois et réglementations en vigueur. Parmi les mesures que nous appliquons pour assurer un niveau élevé de sécurité en termes de gestion des données à caractère personnel figurent, entre autres, les suivantes :

- Pseudonymisation - nous traitons vos données à caractère personnel de manière à ce qu'elles ne puissent plus être attribuées à une personne spécifique sans l'utilisation d'informations supplémentaires. Ces informations supplémentaires sont conservées séparément et font l'objet de mesures techniques et organisationnelles spécifiques afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable ;
- Cryptage - nous appliquons des méthodes cryptographiques qui convertissent certaines informations ou données en un code qui les rend illisibles pour les utilisateurs non autorisés.;
- Minimisation - les données à caractère personnel que nous vous demandons sont adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles ces données sont traitées;
- Contrôle interne strict de l'accès à vos données personnelles - l'accès à vos données personnelles n'est autorisé qu'à nos employés qui ont besoin de cette vérification pour exercer correctement leurs fonctions professionnelles ;
- Tests de résistance - nous effectuons régulièrement des analyses et des tests de résistance afin d'identifier les failles de sécurité potentielles et d'appliquer les mesures correctives nécessaires pour y remédier ;

Veiller à l'application permanente des principes d'intégrité, de confidentialité et de formation de tous nos employés.

Nous maintenons des plans de sécurité et de réponse aux incidents en cas d'incident physique ou technique afin de traiter ce problème en temps opportun et de limiter tout effet négatif d'un tel incident. Bien que nous nous efforcions de protéger vos données à caractère personnel, nous ne pouvons pas garantir que nos mesures de protection empêcheront toute tentative non autorisée d'accès, d'utilisation ou de divulgation de données à caractère personnel.

Nous vous rappelons que vous jouez un rôle essentiel dans la protection de vos données personnelles. Lorsque vous vous inscrivez à nos services, il est important de choisir un mot de passe suffisamment long et complexe, de ne pas révéler ce mot de passe à des tiers et de nous avertir immédiatement si vous avez connaissance d'un accès ou d'une utilisation non autorisés de votre compte. Si vous pensez que les données de connexion à votre compte ont été ou pourraient avoir été exposées, vous pouvez modifier votre mot de passe à tout moment sur notre site web et contacter immédiatement notre service clientèle. Compte tenu de la nature des technologies de communication et de traitement de l'information, nous ne pouvons pas garantir que les informations transmises par l'intermédiaire d'Internet seront totalement à l'abri d'une intrusion par d'autres personnes.

20. MODIFICATIONS DE LA PRÉSENTE POLITIQUE DE PROTECTION DE LA VIE PRIVÉE

Nous pouvons modifier la présente politique de confidentialité de temps à autre en publiant la version mise à jour sur notre site web. Les lois, les réglementations et les normes industrielles évoluent, ce qui peut rendre ces modifications nécessaires, ou nous pouvons apporter des changements à nos activités. Nous vous conseillons de consulter régulièrement cette page afin de rester informé et de vous assurer que vous êtes d'accord avec les changements. Si les changements sont importants, nous vous en informerons de manière plus visible, par exemple en vous envoyant une notification par courrier électronique ou par l'intermédiaire des services. Si vous n'êtes pas d'accord avec les modifications apportées à la présente politique de confidentialité, vous devez cesser d'utiliser nos services. Si nous modifions la présente politique de confidentialité d'une manière qui affecte la façon dont nous utilisons vos données à caractère personnel, nous vous informerons des choix qui s'offrent à vous à la suite de ces modifications.

21. VIOLATIONS DES DONNEES A CARACTERE PERSONNEL

Le RGPD impose à toutes les organisations l'obligation de signaler certains types de violations de données à caractère personnel à l'autorité de contrôle compétente. L'entreprise est tenue de le faire dans les 72 heures après avoir pris

connaissance de la violation, dans la mesure du possible en suivant son cadre de signalement et de gestion des violations de la sécurité des données affectant les données personnelles ou sensibles détenues par l'entreprise.

Si la violation est susceptible d'entraîner un risque élevé d'atteinte aux droits et libertés des personnes, l'entreprise est tenue d'en informer également les personnes concernées dans les plus brefs délais.

Les procédures ci-dessous ont pour but de fournir un cadre pour le signalement et la gestion des violations de la sécurité des données affectant les données personnelles ou sensibles détenues par l'entreprise.

Une violation de données à caractère personnel est définie comme ayant le potentiel d'affecter la confidentialité, l'intégrité ou la disponibilité des données à caractère personnel détenues par l'entreprise sous quelque forme que ce soit. De telles violations peuvent se produire pour un certain nombre de raisons, notamment:

- La divulgation de données confidentielles à des personnes non autorisées;
- Perte ou vol de données et/ou de l'équipement sur lequel les données sont stockées;
- Contrôles inappropriés permettant l'utilisation non autorisée des informations;
- Les atteintes aux systèmes informatiques et à la sécurité de l'entreprise;
- L'accès non autorisé aux systèmes informatiques, par exemple le piratage;
- Virus ou autres attaques de sécurité;
- Les atteintes à la sécurité physique des lieux où sont conservées les données;
- Laisser le matériel informatique sans surveillance, ce qui permet un accès non autorisé;
- Courriels contenant des données personnelles envoyés par erreur au mauvais destinataire.

22. MENTIONS LEGALES

L'entreprise peut divulguer vos informations personnelles identifiables comme l'exigent les règles et réglementations et lorsque l'entreprise estime que la divulgation est nécessaire pour protéger ses droits et/ou pour se conformer à une procédure, à une ordonnance d'un tribunal, à une procédure légale signifiée ou en vertu d'un organisme gouvernemental, intergouvernemental ou d'autres organismes de réglementation.

L'entreprise n'est pas responsable de l'utilisation abusive ou de la perte d'informations personnelles ou autres sur le(s) site(s) web de l'entreprise auquel(s) l'entreprise n'a pas accès ou sur lequel(s) elle n'exerce pas de contrôle. La Société ne sera pas responsable de l'utilisation illégale ou non autorisée de vos informations personnelles en raison d'une mauvaise utilisation ou d'une perte de

vos mots de passe, d'une intervention négligente ou malveillante et/ou autre de votre part ou en raison de vos actes ou omissions ou de ceux d'une personne autorisée par vous (que cette autorisation soit permise ou non par les conditions de notre relation juridique avec vous).

23. VERSION DE REFERENCE

La présente politique peut être traduite en plusieurs langues. En cas d'incohérence entre les différentes versions linguistiques, la version anglaise prévaut.

Dernière version: décembre 2023

PRIVACYBELEID

OPTINITI – 26/12/2023

1. INLEIDING

Dit privacybeleid beschrijft en informeert bezoekers, klanten (potentiële en huidige) en werknemers van onze klanten, hierna "de Betrokkene", hoe OPTINITI SRL (in dit beleid aangeduid als "wij", "ons", "Optiniti", "de Onderneming" of "de Firma"), de aan haar verstrekte informatie gebruikt en beschermt en, in het bijzonder, maar niet uitsluitend, wanneer de Betrokkene de site gebruikt die toegankelijk is via de volgende link: <https://www.optiniti-group.com/>; hierna "de Website", of wanneer de Betrokkene een beroep doet op of gebruik maakt van de door Optiniti aangeboden diensten.

Wij verkrijgen of gebruiken uw persoonsgegevens enkel en alleen voor het leveren, onderhouden en verbeteren van onze diensten en zoals anderszins vereist door de wet. Wij verkrijgen en bewaren persoonsgegevens om verschillende incentiveplannen te beheren die bestemd zijn voor werknemers van onze klanten.

Dit beleid schetst hoe wij dergelijke informatie beheren om ervoor te zorgen dat wij onze verplichtingen nakomen om de privacy van onze klanten te respecteren en dat al deze informatie vertrouwelijk blijft. Deze bindende verplichtingen vloeien voort uit het wettelijke en reglementaire kader voor de verwerking en bescherming van gegevens in België en in het bijzonder de Algemene Verordening Gegevensbescherming (GDPR) (EU) 2016/679 en de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens en voor het vrije verkeer van dergelijke gegevens Wet van 2018 (de "Wet") die werd aangenomen voor de effectieve uitvoering van een aantal bepalingen van de GDPR.

2. WIE ZIJN WE?

Optiniti, met maatschappelijke zetel in België, Avenue Louise 500, B-142, 1050 Brussels (BTW BE07792213945) is de verwerkingsverantwoordelijke (die verantwoordelijk is voor het bepalen van het doel waarvoor en de wijze waarop uw persoonsgegevens worden gebruikt).

Optiniti SRL

E-mail: support@optiniti-group.com

De verwerkingsverantwoordelijke zorgt voor de juistheid en relevantie van de verzamelde en verwerkte persoonsgegevens. Bovendien zal hij ervoor zorgen dat hij voldoet aan de toepasselijke regelgeving en dit privacybeleid.

Wij zetten ons in om het juiste te doen als het gaat om hoe we uw persoonsgegevens verzamelen, gebruiken en beschermen. Daarom hebben wij dit privacybeleid ("Beleid") ontwikkeld, dat:

- de verschillende manieren beschrijft waarop je met ons communiceert en de soorten persoonsgegevens die wij verzamelen;
- uitlegt waarom we de gegevens die we verzamelen, gebruiken;
- uitlegt wanneer en waarom wij persoonsgegevens delen binnen Optiniti en met andere
- organisaties (hieronder gedefinieerd); en
- uitlegt welke rechten en keuzes je hebt als het gaat om jouw persoonsgegevens.

3. WAT BEDOELEN WE MET PERSOONSGEGEVENS?

Persoonsgegevens zijn alle informatie over jou of gegevens die kunnen worden gebruikt om je direct of indirect te identificeren.

In het algemeen is het mogelijk de Website te bezoeken zonder persoonsgegevens te verstrekken. De Betrokkene is in ieder geval geenszins verplicht zijn of haar gegevens aan het bedrijf door te geven.

In bepaalde situaties waarin geen informatie wordt verstrekt, is het echter mogelijk dat de Betrokkene niet kan genieten van de gevraagde diensten. Om de Betrokkene in staat te stellen om van de door het bedrijf aangeboden diensten te genieten, kan het bedrijf er in bepaalde gevallen toe gebracht worden jou of je werkgever te vragen om je naam/namen, voornaam/voornamen, geslacht, taal, nationaliteit, adres, rijksregisternummer, telefoonnummer, e-mailadres, hierna "persoonsgegevens". Door deze informatie te verstrekken, stemt de Betrokkene uitdrukkelijk in met de verwerking ervan door Optiniti voor de doeleinden vermeld in punt 6 hieronder en voor de doeleinden vermeld op het moment van elk verzoek.

In overeenstemming met de Algemene Verordening Gegevensbescherming (GDPR) van 14 april 2016, brengt het bedrijf je op de hoogte van het volgende:

Optiniti kan je andere documentatie vragen die nodig is voor het effectieve beheer van het incentiveplan waarvan je deel zou uitmaken.

4. WAT VOOR INFORMATIE HEBBEN WIJ NODIG EN WAAROM?

Wanneer je onze website of ons Platform bezoekt via de website, kunnen wij persoonsgegevens over jou verzamelen via je navigatie op de website en je verbinding met het Platform.

Wij verwerken de persoonsgegevens die wij van jou hebben ontvangen als onderdeel van de contractuele relatie die wij hebben met je werkgever of ten

behoefte van legitieme belangen die Optiniti nastreeft. Wij kunnen ook gegevens verwerken die wij rechtmatig hebben ontvangen uit openbaar beschikbare bronnen en identificatiedatabanken. In principe zijn wij verplicht of zouden wij uw persoonsgegevens nodig hebben:

- Bij het aangaan en onderhouden van een contractuele relatie zijn wij verplicht persoonsgegevens van jou te verzamelen om ons in staat te stellen je identiteit vast te stellen en te verifiëren. Daartoe vragen wij je om persoonsgegevens, waaronder, maar niet uitsluitend, je volledige naam, land van verblijf, adres, geboortedatum, nationaliteit, rijksregisternummer, e-mailadres of andere contactgegevens;
- Om je transacties te vergemakkelijken, kunnen wij je IBAN-gegevens en andere betalingsverwerkingsinformatie verwerken zoals gevraagd door de respectieve betalingsdienstaanbieders;
- Om de geschiktheid van onze Diensten voor jouw omstandigheden en ervaring te beoordelen, kunnen wij om aanvullende informatie vragen zoals, maar niet beperkt tot, software-ervaring, werkgelegenheidsgegevens, kennis van en ervaring met financiële diensten en producten;

Wij kunnen ook informatie over jou verzamelen en moeten deze verwerken via je gebruik van ons platform. Dergelijke informatie kan onder meer omvatten:

- Het Internet Protocol (IP) adres dat wordt gebruikt om je computer met het internet te verbinden, je inloggegevens, je geografische locatie, je browser en browser plug-in type en versie, uw besturingssysteem en platform, en andere indirecte persoonsgegevens. Wanneer wij dergelijke informatie verwerken, streven wij ernaar deze altijd op geaggregeerde en geanonimiseerde basis te gebruiken;
- Alle andere persoonlijke informatie die nodig kan zijn om te voldoen aan de toepasselijke regels; en
- Alle andere persoonlijke informatie die nodig is om geschillen te beslechten of een juridische verdediging voor te bereiden.

5. HOE WORDEN JE PERSOONSGEGEVENS VERZAMELD?

Wij verzamelen de meeste van deze persoonsgegevens rechtstreeks van uw werkgever, via onze beveiligde software om documenten te delen en samen te werken aan content / Platform. Echter, in sommige gevallen, kunnen we jou of je werkgever via e-mail of via ons invulformulier om aanvullende informatie vragen en ook onze eigen gegevens en informatie uit andere bronnen gebruiken om te voldoen aan wettelijke en regelgevende verplichtingen.

De verwerking en opslag van je persoonlijke gegevens is noodzakelijk om je de diensten te leveren die met je werkgever zijn overeengekomen en die zijn beschreven in de samenwerkingsovereenkomst tussen Optiniti en je werkgever en om te voldoen aan onze wettelijke verplichtingen. Als je ervoor kiest sommige van de gevraagde gegevens niet aan ons te verstrekken, kunnen wij je mogelijk

niet onboarden als een nieuwe begunstigde van een incentiveplan of kunnen wij de dienstverlening in het kader van een bestaand plan stopzetten.

Wij houden de informatie zo actueel mogelijk en zullen alle gegevens, zoals je adres, onmiddellijk wijzigen wanneer je ons meedeelt dat zij zijn gewijzigd.

Persoonlijke gegevens die door Optiniti kunnen worden verwerkt omvatten elk type elektronische communicatie zoals brieven, e-mails, telefoongesprekken, fiscaal identificatienummer en alle gerelateerde fiscale informatie, alle persoonlijke informatie die voortvloeit uit de "Know Your-Customer" en "Anti Money Laundering" controles die door Optiniti worden uitgevoerd krachtens de toepasselijke wetgeving met betrekking tot de strijd tegen het witwassen van geld en de financiering van terrorisme.

Je gebruik van het Platform omvat de geautomatiseerde verzameling van bepaalde soorten informatie, waarvan sommige als persoonsgegevens kunnen worden beschouwd. Deze informatie omvat: IP-adres, browsertype en besturingssysteem.

Daarnaast maakt de Website gebruik van een reeks cookies om uw ervaring te verbeteren en te personaliseren. Meer informatie hierover vind je in ons cookiebeleid.

6. WAAROM HEBBEN WIJ DEZE INFORMATIE NODIG EN OP WELKE JURIDISCHE GRONDSLAG WORDEN DE GEGEVENS VERWERKT?

Rechtmatigheid van de verwerking

Wij zullen je persoonsgegevens verwerken (inclusief verzamelen, gebruiken, opslaan en overdragen, indien van toepassing)

- voor het effectieve beheer van de incentiveplannen die zijn beschreven in de Samenwerkingsovereenkomst die is gesloten tussen je werkgever als klant en Optiniti (de "Diensten");
- voor de naleving van wettelijke en regelgevende verplichtingen waaraan Optiniti is onderworpen (met inbegrip van maar niet beperkt tot de verplichtingen die voortvloeien uit de MIFID 2-verordening, wettelijke verplichtingen tegen het witwassen van geld en het tegengaan van de financiering van terrorisme, alle toepasselijke belastingwetgeving, enz. Voorbeelden van dergelijke wettelijke verplichtingen zijn onder meer: rapportageverplichtingen aan de EMIR-autoriteiten; het verstrekken van informatie aan de financiële criminaliteitsautoriteiten over verdachte witwastransacties of in het kader van financiële strafprocedures; het verstrekken van informatie aan de belastingautoriteiten. Merk op dat wij, om aan sommige van de bovenstaande verplichtingen te voldoen, gebruik kunnen maken van geautomatiseerde besluitvorming en

profilering, terwijl je om menselijke tussenkomst kunt verzoeken; je zal echter geen bezwaar kunnen maken tegen een dergelijke verwerking.

- Indien de verwerking van persoonsgegevens noodzakelijk is voor de doeleinden van de legitieme belangen die Optiniti nastreeft - bijvoorbeeld wanneer dit noodzakelijk is - om ervoor te zorgen dat we u de best mogelijke diensten en informatie kunnen bieden en om onze producten in uw belang te blijven verbeteren.
- In het kader van je toestemming - bijvoorbeeld voor marketing- en promotiedoeleinden. Als je ons toestemming hebt verleend om je persoonsgegevens te verwerken voor marketingdoeleinden, zal de verwerking alleen plaatsvinden in overeenstemming met de doeleinden die in de toestemmingsverklaring zijn uiteengezet en in de mate die daarin is overeengekomen. Je kan te allen tijde elke gegeven toestemming met toekomstige werking laten intrekken.

Doeleinden

Optiniti zal je directe persoonsgegevens (zoals je naam, geboortedatum, ID enz.) en indirecte persoonsgegevens (zoals analytische en trackinggegevens) verwerken en analyseren in combinatie met uw gebruik van je account voor de doeleinden van:

- het leveren van de door je werkgever gevraagde en met betrekking tot de Samenwerkingsovereenkomst uitgevoerde Diensten, waaronder onder meer;
 - o het verifiëren van je identiteit, het openen en beheren van je account op het Platform;
 - o het voldoen aan onze wettelijke verplichtingen;
 - o het verwerken van je verzoeken met betrekking tot de Diensten
 - o het beheren van klantrelaties door middel van elektronische, telefonische of chatcommunicatie, het aangaan en uitvoeren van transacties met financiële instrumenten;
 - o het uitvoeren van een controle op risicobeheer, gegevensanalyse en globaal toezicht op je lopende behoeften en het verbeteren van de aan jou aangeboden diensten;
 - o het verbeteren en personaliseren van onze Diensten om je ervaring te verbeteren
 - o het voorkomen van misbruik en fraude, het aantonen van zakelijke transacties en communicatie; het beheren van het toezicht op transacties en het bewaken en naleven van rapporteringsverplichtingen; het beheren van risico's, geschillen, klachten, rechtszaken of in het kader van vervolging;
- het verzenden van de elektronische nieuwsbrief aan de Betrokkene

- het verstrekken van de door de Betrokkene gevraagde informatie of diensten (door aanwezigheid op de operationele sites, per e-mail, per telefoon of per post) en op maat van de Betrokkene, en meer in het bijzonder :
- de verwerking en opvolging van prijs- en/of informatieaanvragen aan het bedrijf;
- de presentatie van de door de onderneming aangeboden en geleverde diensten
- statistieken over de bezoeken aan de Website van de onderneming;
- om informatie te verzamelen waarmee de onderneming de Website, producten en diensten kan verbeteren (met name door middel van cookies);
- aan Google Analytics, door middel van cookies, zoals hieronder vermeld en/of in de disclaimer die op de website van de onderneming kan worden geraadpleegd via de volgende link: <https://optiniti-group.odoo.com/cookie-policy>

7. WIE ZIJN DE ONTVANGERS VAN JE PERSOONSGEGEVENS?

Je persoonsgegevens worden ontvangen en verwerkt door die medewerkers van Optiniti die deze nodig hebben voor de uitvoering van contractuele, wettelijke en reglementaire verplichtingen. Verder kunnen wij, voor zover wij een dergelijke openbaarmaking of overdracht noodzakelijk achten voor het voldoen aan de hierboven uiteengezette doeleinden, bekendmaken aan de volgende ontvangers:

- Andere bedrijven die samenwerken met Optiniti, zoals de Software Provider(s). Deze gegevens kunnen worden doorgegeven om ons in staat te stellen je een volledige dienstverlening te bieden, waarbij andere bedrijven binnen de volledige dienstverlening onderdelen uitvoeren, zoals IT-onderhoud of ondersteunende diensten;
- Alle advocaten, externe auditors of adviseurs, professionele consultants, kredietreferentiebureaus, notarissen, deurwaarders, evenals alle rechtbanken, regelgevende, overheids-, administratieve of andere officiële instanties zoals overeengekomen of wettelijk vereist, wanneer deze openbaarmaking noodzakelijk is
 - (i) om te voldoen aan enige toepasselijke wet- of regelgeving;
 - (ii) om toepasselijke voorwaarden of beleid af te dwingen;
 - (iii) om de veiligheid of integriteit van onze diensten te beschermen; en
 - (iv) om onze rechten en belangen te beschermen;
- Externe dienstverleners of gegevensverwerkers die IT-diensten, identiteitscontroles, bank- en betalingsverwerkingsdiensten of andere

diensten aan Optiniti leveren, die alleen gemachtigd zijn om je persoonsgegevens te verwerken strikt voor het leveren van deze diensten en in overeenstemming met onze instructies. Indien van toepassing, zullen wij met dergelijke externe dienstverleners de relevante contractuele overeenkomsten of de standaardclausules inzake gegevensbescherming aangaan die vereist zouden zijn onder de relevante wetgeving inzake gegevensbescherming om de naleving van onze instructies te waarborgen; en

- Derden in het kader van fusies en overnames, op voorwaarde dat de potentiële koper of verkoper ermee instemt uw persoonsgegevens te respecteren op een manier die in overeenstemming is met ons Privacybeleid.

Wij zullen van elke entiteit aan wie wij je informatie bekendmaken of die deze namens ons verkrijgt, eisen dat zij de vertrouwelijkheid ervan waarborgt en deze behandelt in overeenstemming met het legitieme doel waarvoor zij toegang heeft en in overeenstemming met de toepasselijke wetgeving inzake gegevensbescherming.

Wij zullen uw informatie niet delen of verkopen aan derden voor hun eigen onafhankelijke marketing of zakelijke doeleinden zonder jouw toestemming.

Informatie internationaal overdragen

Persoonsgegevens kunnen worden bewaard in onze kantoren en bij externe bureaus, dienstverleners, vertegenwoordigers, accountants, advocaten en agenten, zoals hierboven beschreven. Sommige van deze derden kunnen buiten de EU en de Europese Economische Ruimte (EER) gevestigd zijn.

Volgens de gegevensbeschermingswetgeving mogen wij je persoonsgegevens alleen doorgeven aan een land of internationale organisatie buiten de EU/EER wanneer:

- de Europese Commissie heeft besloten dat het specifieke land of de internationale organisatie een passend niveau van bescherming van persoonsgegevens waarborgt (bekend als een "adequaateitsbesluit");
- er passende waarborgen zijn, samen met afdwingbare rechten en doeltreffende rechtsmiddelen voor de betrokkenen; of
- de wetgeving inzake gegevensbescherming voorziet in een specifieke uitzondering.

Adequaateitsbesluit

Wij kunnen je persoonsgegevens doorgeven aan bepaalde landen, op basis van een adequaateitsbesluit. De lijst van landen waarvoor een adequaateitsbesluit geldt, zal van tijd tot tijd veranderen. Wij zullen altijd trachten te vertrouwen op een adequaateitsbesluit, wanneer dat bestaat.

Andere landen waaraan wij waarschijnlijk persoonsgegevens zullen doorgeven, komen niet in aanmerking voor een adequaateitsbesluit. Dit betekent niet

noodzakelijk dat zij de persoonsgegevens slecht beschermen, maar wij moeten alternatieve gronden voor het doorgeven van de persoonsgegevens onderzoeken, zoals passende waarborgen of een beroep doen op een uitzondering, zoals hieronder uiteengezet.

De gegevens kunnen worden verwerkt door personeel dat voor ons of voor een van onze leveranciers werkt en zich buiten de EU en/of de EER bevindt. Dit personeel kan bijvoorbeeld betrokken zijn bij de uitvoering van onze ondersteunende diensten. Wij zullen alle nodige stappen ondernemen om ervoor te zorgen dat je persoonsgegevens veilig en in overeenstemming met dit Privacybeleid worden behandeld. We hebben passende waarborgen aangenomen om ze te beschermen.

Overdracht met passende waarborgen

Wanneer er geen besluit inzake adequaatheid is, kunnen wij je persoonsgegevens naar een ander land overdragen indien wij ervan overtuigd zijn dat de overdracht voldoet aan de wetgeving inzake gegevensbescherming, er passende waarborgen zijn en er voor jou, als Betrokkene, afdwingbare rechten en doeltreffende rechtsmiddelen beschikbaar zijn.

De waarborgen omvatten gewoonlijk het gebruik van wettelijk goedgekeurde standaardcontractbepalingen inzake gegevensbescherming. Op die manier maken wij bindende afspraken met dergelijke derden, zodat je gegevens volgens dezelfde normen worden beschermd als in de EU en de EER.

8. HOE LANG WORDEN JE GEGEVENS BEWAARD?

Wij verwerken je persoonsgegevens voor de gehele duur van de Samenwerkingsovereenkomst die je werkgever met ons heeft gesloten en voor een periode van tien (10) jaar na beëindiging van de Overeenkomst om te voldoen aan de toepasselijke antiwitwaswetgeving en wettelijke bewaarplichten. Verder worden persoonsgegevens niet langer bewaard dan de tijd die nodig is voor de doeleinden van de verwerking ervan, behoudens de algemene wettelijke verjaringstermijnen en de genoemde bewaartermijn wanneer de toepasselijke wetgeving vereist dat de persoonsgegevens gedurende een bepaalde periode na de beëindiging van onze zakelijke relatie met jou worden bewaard.

9. WAT ZIJN JE RECHTEN MET BETREKKING TOT DE VERWERKING VAN JE PERSOONSGEGEVENS?

Je hebt het recht op:

Recht op toegang en mededeling van gegevens

De Betrokkene heeft het recht om de persoonsgegevens die het bedrijf over hem/haar bewaart, in te zien en te raadplegen. De Betrokkene kan ook nagaan hoe het bedrijf de gegevens heeft verkregen en aan wie ze werden meegedeeld. De Betrokkene kan ook een kopie vragen van deze persoonsgegevens tijdens de verwerking.

Gelet op de verplichting van het bedrijf tot veiligheid en vertrouwelijkheid bij de verwerking van persoonsgegevens, wordt het verzoek van de Betrokkene om toegang tot en raadpleging van de gegevens verwerkt op voorwaarde dat de identiteit wordt aangetoond, met name door voorlegging van een elektronische of papieren kopie (voorzien van een handtekening) van zijn identiteitskaart tijdens de geldigheidsduur daarvan. Het verzoek is in elk geval kosteloos voor de Betrokkene.

Het bedrijf kan zich echter verzetten tegen verzoeken die duidelijk misbruikt of ongegrond zijn (bijvoorbeeld door hun aantal of hun repetitieve of systematische aard).

Recht op correctie van gegevens

Volgens de Europese verordening kan de Betrokkene verzoeken om rectificatie, bijwerking of verwijdering van gegevens die hem of haar betreffen en die mogelijk onjuist, foutief, onvolledig of verouderd zijn.

Recht van verzet

De betrokkene heeft in de volgende twee situaties het recht bezwaar te maken tegen de verwerking van gegevens

- wanneer de uitoefening van dit recht gebaseerd is op legitieme gronden of
- wanneer de uitoefening van dit recht tot doel heeft te voorkomen dat de verzamelde gegevens voor commerciële prospectiedoeleinden worden gebruikt.

Recht op beperking

De Betrokkene kan de onderneming verzoeken de verwerking van zijn/haar persoonsgegevens in bepaalde omstandigheden te beperken, bijvoorbeeld wanneer je de juistheid van de persoonsgegevens betwist, gedurende een periode om Optiniti in staat te stellen de juistheid van je persoonsgegevens te controleren of in het geval dat je van mening bent dat de verwerking onwettig is. Een dergelijk bezwaar kan echter niet voorkomen dat wij je persoonsgegevens opslaan.

Recht op wissen

De Betrokkene heeft het recht om de verwijdering te vragen en te verkrijgen van gegevens over hem/haar die in het bezit zijn van het bedrijf.

Het bedrijf zal voldoen aan het verzoek van de betrokkene indien :

- de persoonsgegevens niet langer noodzakelijk zijn voor de doeleinden waarvoor ze zijn verzameld;

- de verwerking van de gegevens uitsluitend gebaseerd was op de toestemming van de betrokkene en de betrokkene zijn toestemming intrekt;
- de betrokkene maakt om gegronde redenen bezwaar tegen de verwerking.

In elk geval kan het verzoek tot wissen door het bedrijf worden geweigerd indien het verzoek noodzakelijk is voor de uitoefening of verdediging van wettelijke rechten of voor de naleving van een wettelijke of contractuele verplichting van het bedrijf.

Recht op gegevensoverdraagbaarheid

De Betrokkene kan verzoeken dat zijn of haar persoonsgegevens worden overgedragen aan een voor de verwerking verantwoordelijke die identiek is aan het bedrijf. De Betrokkene kan daarom vragen dat de gegevens in een gestructureerd, algemeen gebruikt en voor de computer leesbaar formaat aan het bedrijf worden overgedragen.

Hoe je rechten uitoefenen

De bovengenoemde rechten kunnen worden uitgeoefend door een brief te sturen naar het adres van de onderneming of door een e-mail te sturen naar het volgende adres: support@optiniti-group.com.

Antwoordtermijn

Het bedrijf zal op het verzoek van de Betrokkene reageren op dezelfde wijze als waarop de Betrokkene zijn recht heeft uitgeoefend.

Het bedrijf verbindt zich ertoe op elk verzoek om toegang, rectificatie of verzet, verwijdering of elk ander bijkomend verzoek om informatie te antwoorden binnen een redelijke termijn en in elk geval binnen een maximum van 1 maand na ontvangst van je verzoek.

Afhankelijk van de complexiteit van het verzoek kan de antwoordtermijn worden verlengd tot 3 maanden, overeenkomstig de toepasselijke Europese verordening.

10. HOE BEHEREN EN BESCHERMEN WIJ JOUW PERSOONSGEGEVENS?

Wij doen alle moeite en passen de hoogste technische en organisatorische normen toe om ervoor te zorgen dat je persoonsgegevens worden beveiligd en vertrouwelijk blijven. Alle persoonlijke gegevens die je ons verstrekt, worden opgeslagen op beveiligde servers, en wij gebruiken strenge procedures om je te beschermen tegen verlies, misbruik, onbevoegde toegang, wijziging, openbaarmaking of vernietiging van je persoonlijke gegevens. Wij beschermen je persoonsgegevens door fysieke, elektronische en procedurele waarborgen te handhaven in overeenstemming met de toepasselijke wet- en regelgeving. Een

deel van de maatregelen die wij toepassen om een hoog niveau van beveiliging te bieden op het gebied van het beheer van persoonsgegevens zijn onder meer:

- Pseudonimisering - wij verwerken je persoonsgegevens op zodanige wijze dat deze niet meer aan een specifieke persoon kunnen worden toegeschreven zonder het gebruik van aanvullende informatie, welke aanvullende informatie apart wordt bewaard en onderworpen is aan specifieke technische en organisatorische maatregelen om ervoor te zorgen dat de persoonsgegevens niet worden toegeschreven aan een geïdentificeerde of een identificeerbare natuurlijke persoon;
- Encryptie - wij passen cryptografische methoden toe die bepaalde informatie of gegevens omzetten in een code om ze onleesbaar te maken voor onbevoegde gebruikers;
- Minimalisering - de persoonsgegevens die wij van jou vragen zijn adequaat, relevant en alleen beperkt tot wat noodzakelijk is in verband met de doeleinden waarvoor deze gegevens worden verwerkt;
- Strikte interne controle op de toegang tot jouw persoonsgegevens - toegang tot jouw persoonsgegevens is alleen toegestaan aan onze medewerkers die deze controle nodig hebben om hun professionele taken naar behoren uit te voeren;
- Penetratietests - wij voeren regelmatig scans en penetratietests en -diensten uit om potentiële beveiligingskwetsbaarheden te identificeren en de relevante remedies toe te passen om deze te verhelpen;
- Het voortdurend toepassen van integriteit, vertrouwelijkheid en opleiding van al onze medewerkers.

Wij hanteren beveiligings- en incidentbestrijdingsplannen voor het geval zich een fysiek of technisch incident voordoet om dit tijdig af te handelen en eventuele negatieve gevolgen van een dergelijk incident te beperken. Hoewel wij hard werken om je persoonsgegevens te beschermen, kunnen wij niet garanderen dat onze beveiligingen elke ongeoorloofde poging tot toegang, gebruik of openbaarmaking van persoonsgegevens zullen voorkomen.

Besef dat je een essentiële rol speelt in de bescherming van je eigen persoonsgegevens. Wanneer je zich bij onze diensten registreert, is het belangrijk een wachtwoord van voldoende lengte en complexiteit te kiezen, dit wachtwoord niet aan derden bekend te maken en ons onmiddellijk op de hoogte te stellen als je je bewust wordt van ongeoorloofde toegang tot/gebruik van je account. Als je denkt dat de inloggegevens van je account zijn of kunnen zijn blootgesteld, kan je jouw wachtwoord te allen tijde wijzigen via onze Website en onmiddellijk contact opnemen met onze klantenservice. Gezien de aard van de communicatie- en informatieverwerkingstechnologie kunnen wij niet garanderen dat informatie die via het internet wordt verzonden, volledig veilig is voor inbraak door anderen.

11. WIJZIGINGEN AAN DIT PRIVACYBELEID

Wij kunnen dit Privacybeleid van tijd tot tijd wijzigen door de bijgewerkte versie op onze Website te plaatsen. Wetten, voorschriften en industriënormen evolueren, waardoor deze wijzigingen noodzakelijk kunnen zijn, of wij kunnen wijzigingen aanbrengen in ons bedrijf. Wij raden je aan deze pagina regelmatig te bekijken om op de hoogte te blijven en ervoor te zorgen dat je tevreden bent met eventuele wijzigingen. Als de wijzigingen aanzienlijk zijn, zullen wij je hierover informeren, zoals bv. Via een kennisgeving per e-mail of via de Diensten. Als je het niet eens bent met de wijzigingen in dit Privacybeleid, moet je stoppen met het gebruik van onze diensten. Als wij dit Privacybeleid wijzigen op een manier die van invloed is op de manier waarop wij jouw persoonsgegevens gebruiken, zullen wij je informeren over de keuzes die je als gevolg van deze wijzigingen hebt.

12. INBREUKEN IN VERBAND MET PERSOONS-GEGEVENS

De GDPR voert een verplichting in voor alle organisaties om bepaalde soorten inbreuken op persoonsgegevens te melden aan de relevante toezichthoudende autoriteit. De Vennootschap is verplicht dit te doen binnen 72 uur na kennisname van de inbreuk, waar mogelijk volgens haar kader voor het melden en beheren van inbreuken op de gegevensbeveiliging die betrekking hebben op persoonlijke of gevoelige gegevens waarover de Vennootschap beschikt.

Als de inbreuk waarschijnlijk leidt tot een hoog risico op negatieve gevolgen voor de rechten en vrijheden van personen, moet de onderneming ook deze personen/betrokkenen zonder onnodige vertraging informeren.

De onderstaande procedures bieden een kader voor het melden en beheren van inbreuken op de gegevensbeveiliging die betrekking hebben op persoonlijke of gevoelige gegevens waarover de onderneming beschikt.

Een inbreuk op persoonsgegevens wordt gedefinieerd als een inbreuk op de vertrouwelijkheid, integriteit of beschikbaarheid van persoonsgegevens die het bedrijf in welk formaat dan ook bewaart. Dergelijke inbreuken kunnen om verschillende redenen plaatsvinden, waaronder

- De bekendmaking van vertrouwelijke gegevens aan onbevoegden;
- Verlies of diefstal van gegevens en/of apparatuur waarop gegevens zijn opgeslagen;
- Ongeschikte controles die onbevoegd gebruik van informatie mogelijk maken;
- Inbreuken op de IT-systemen en beveiliging van het bedrijf;
- Onbevoegde toegang tot computersystemen, bijvoorbeeld hacken;
- Virussen of andere beveiligingsaanvallen;
- Inbreuken op de fysieke beveiliging waar gegevens worden bewaard;
- Het onbeheerd achterlaten van IT-apparatuur waardoor onbevoegden toegang krijgen;

- E-mails met persoonlijke gegevens die per ongeluk naar de verkeerde ontvanger zijn gestuurd.

13. JURIDISCHE DISCLAIMER

Het Bedrijf kan je persoonlijk identificeerbare informatie openbaar maken zoals vereist door regels en voorschriften en wanneer het Bedrijf van mening is dat openbaarmaking noodzakelijk is om onze rechten te beschermen en/of te voldoen aan een procedure, een gerechtelijk bevel, een juridisch proces dat wordt gevoerd of op grond van overheids-, intergouvernementele of andere regelgevende instanties.

Het Bedrijf is niet aansprakelijk voor misbruik of verlies van persoonlijke informatie of anderszins op de website(s) van het Bedrijf waartoe het Bedrijf geen toegang of controle heeft. Het Bedrijf is niet aansprakelijk voor onwettig of ongeoorloofd gebruik van je persoonsgegevens door misbruik of verkeerde plaatsing van je wachtwoorden, nalatig of kwaadwillig ingrijpen en/of anderszins door jou of door je handelen of nalaten of een door jou gemachtigd persoon (ongeacht of die machtiging is toegestaan door de voorwaarden van onze rechtsverhouding met jou of niet).

14. TOONAANGEVENDE VERSIE

Dit Beleid kan in verschillende talen worden vertaald. Als er tegenstrijdigheden zijn tussen verschillende taalversies, heeft de Engelstalige versie voorrang.

Laatst bijgewerkt: december 2023

PRIVACY POLICY

OPTINITI – 26/12/2023

1. INTRODUCTION

This privacy policy sets out and informs visitors, customers (potential and actual) and customer's worker, hereinafter "Data subject", how OPTINITI SRL (referred to in this policy as "we", "us", "Optiniti", "the Company" or "the Firm"), uses and protects the information provided to it and, in particular, but not exclusively, when Data subject uses this site accessible via the following link: <https://www.optiniti-group.com/>; hereinafter "the Website", or when Data subject calls upon or uses the services offered by Optiniti.

We do not access or use your personal data for any purpose other than in providing, maintaining and improving our services and as otherwise required by law. We obtain and hold personal information in order to manage various incentive plans destined to employees of our clients.

This policy outlines how we manage such information to ensure we meet our obligations to respect our clients' privacy and that all such information remains confidential. These binding obligations derive from the legal and regulatory framework governing the processing and protection of personal data in Belgium and in particular the General Data Protection Regulation (GDPR) (EU) 2016/679 and the Protection of Natural Persons With Regard to the Processing of Personal Data and for the Free Movement of Such Data Law of 2018 (the "Law") which was adopted for the effective implementation of certain provisions of the GDPR.

2. WHO ARE WE?

Optiniti, with registered office in Belgium, Avenue Louise 500, B-142, 1050 Brussels (VAT BE0792213945) is the data controller (who is responsible for determining the purpose and manner in which your personal data is used).

Optiniti SRL

Email: support@optiniti-group.com

The data controller shall ensure the accuracy and relevance of the personal data collected and processed. In addition to the above, it shall ensure that it complies with the applicable regulations and this privacy policy.

We are committed to doing the right thing when it comes to how we collect, use and protect your personal data and is why we've developed this privacy policy ("Policy"), which:

- Sets out the different ways you interact with us and the types of personal data that we collect;
- Explains the reasons why we use the data we collect;
- Explains when and why we will share personal data within Optiniti and with other organisations (defined below); and
- Explains the rights and choices you have when it comes to your personal data.

3. WHAT DO WE MEAN BY PERSONAL DATA?

Personal data is any information relating to you or data that may be used to identify you directly or indirectly.

In general, it is possible to visit the Website without providing any personal information. In any case, the Data subject is in no way obliged to transmit his or her information to the company.

However, in certain situations where information is not provided, it is possible that the Data subject may not be able to benefit from the services requested. Indeed, in order to allow the Data subject to benefit from the services offered by the company, the latter may be led, in certain cases, to ask you or your employer to provide your surname(s), first name(s), gender, language, nationality, address, national registration number, telephone number, e-mail address, hereinafter referred to as "personal information". By providing this information, the Data subject expressly agrees to its processing by Optiniti for the purposes indicated in point 6 below and for the purposes indicated at the time of each request.

In accordance with the General Data Protection Regulation (GDPR) of 14 April 2016, the company informs you that Optiniti may ask you other documentation which may be requested for the effective management of the incentive plan you would be part of.

4. WHAT SORT OF INFORMATION DO WE NEED AND WHY?

When you access our website or our Platform via the website, we may collect personal data about you through your navigation on the website and your connections to the Platform.

We process the personal data that we received from you as part of the contractual relationship that we have with your employer or for the purposes of legitimate interests pursued by Optiniti. We may also process data that we have legitimately

received from publicly available sources and identification databases. In principle, we are obligated or would need your personal data:

- In the course of establishing and maintaining a contractual relationship we are obligated to collect personal information from you to enable us to establish and verify your identity. To do this, we will request personal data which includes, but may not be limited to your full name, country of residence, your address, date of birth, nationality, national registration ID, email address or other contact information;
- To facilitate your transactions, we may process your IBAN details and other payment processing information as requested by the respective payment services providers;
- To assess the appropriateness of our Services to your circumstances and experience, we may ask for additional information such as, but not limited to, software experience, employment details, knowledge and experience in financial services and products;

We may also collect and be required to collect and process information about you through your use of our platform. Such information may include, among others:

- the Internet Protocol (IP) address used to connect your computer to the internet, your login information, your geographic location, your browser and browser plug-in type and version, your operating system and platform, and other indirect personal data. Whenever we process such information, we will aim at always using it in an aggregated and anonymised bases;
- Any other personal information which may be needed to comply with applicable rules; and
- Any other personal information which may be needed to settle any disputes or prepare a legal defence.

5. HOW IS YOUR PERSONAL DATA COLLECTED?

We collect most of this personal data directly from your employer, via our secure content collaboration & file sharing software / Platform¹. However, in some instances:

We may request additional information from you or your employer via email or through our application form, and also use our own records and information from other sources for compliance with legal and regulatory obligations.

¹ The Platform refers to the software from where Beneficiaries can manage their respective Incentive Plans.

The processing and the storage of your personal data is necessary to provide you with the services agreed with your employer which are described in the Collaboration Agreement between Optiniti and your Employer and to comply with our regulatory obligations. If you choose not to provide some of the requested information to us, we may not be able to onboard you as a new beneficiary of incentive plan or to cease services provided under an existing plan.

We keep the information as up to date as possible, and will change any details, such as your address, promptly when you inform us that they have changed.

Personal data that may be processed by Optiniti includes any type of electronic communications such as letters, emails, telephone conversations, tax identification number and any related tax information, any personal information resulting from the 'Know Your-Customer' and 'Anti Money Laundering' checks carried out by Optiniti pursuant to the applicable legislation relating to the fight against money laundering and terrorist financing.

Your use of the Platform and involves the automated collection of certain types of information, some of which may be considered personal information. This information includes: IP address, browser type and operating system.

In addition, the Website uses a range of cookies to improve and personalise your experience. More information about these can be found in our Cookies Policy.

6. WHY DO WE NEED THIS INFORMATION AND ON WHAT LEGAL BASIS IS THE DATA PROCESSED?

Lawfulness of processing

We will process your personal data (including collect, use, store and transfer, if applicable):

- for the effective management of incentive plans depicted in the Collaboration Agreement concluded between your employer as a client and Optiniti (the "Services");
- for compliance with legal and regulatory obligations to which Optiniti is subject (including but not limited to the obligations arising under the MIFID 2 regulation, anti-money laundering and countering terrorist financing regulatory obligations, any applicable tax legislation etc.), EMIR, etc. Examples of such regulatory obligations include, among others: reporting obligations to EMIR authorities; providing information to financial crime authorities of suspicious money-laundering transactions or in the context of financial criminal proceedings; providing information to tax authorities. Please note that in order to meet some of the above requirements we may use automated decision making and profiling, whereas you may request

human intervention, however, you will not be able to object to such processing.

- In case the processing of personal data is necessary for the purposes of the legitimate interests pursued by Optiniti - for example, in it is necessary - to ensure that we provide you with the best services and information we can and to continue improving our products in your best interest.
- Within the scope of your consent – for example, for marketing and promotional purposes. If you have granted us consent to process your personal data for marketing purposes, processing will only take place in accordance with the purposes set out in the declaration of consent and to the extent agreed therein. Any consent given may be revoked at any time by you with future effect.

Purposes

Optiniti will process and analyse your direct personal data (such as your name, date of birth, ID etc.) and indirect personal data (such as analytics and tracking data) in combination with your use of your account for the purposes of:

- providing the Services requested by your employer and carried out in relation to the Collaboration Agreement, including, among others, verify;
 - o verifying your identity, opening and managing your account on the Platform;
 - o meeting our regulatory obligations;
 - o processing your requests related to the Services;
 - o managing client relationships by means of electronic, telephone or chat communication, entering into and executing transactions with financial instruments;
 - o conducting a risk management control, data analysis and global supervision of your ongoing needs and enhancing the services offered to you;
 - o improving and personalising our Services to enhance your experience;
 - o preventing misuse and fraud, demonstrating business transactions and communications; managing transactions surveillance and monitoring and complying with reporting obligations; managing risks, disputes, complaints, litigation or in the context of prosecution;
- sending the electronic newsletter to Data subject;
- providing the information or services requested by the Data subject (by presence on the operating sites, by e-mail, by telephone or by post) and tailored to the Data subject, and more specifically :
- the processing and follow-up of requests for prices and/or information made to the company;
- the presentation of the services offered and provided by the company;
- statistics on visits to the company's website;
- to collect information enabling the company to improve the Website, products and services (in particular by means of cookies);

- to Google Analytics, by means of cookies, as listed below/or in the disclaimer that can be consulted on the company's website via the following link: <https://optiniti-group.odoo.com/cookie-policy>

7. WHO ARE THE RECIPIENTS OF YOUR PERSONAL DATA?

Your personal data is received and processed by those employees of Optiniti that need it for the execution of contractual, legal and regulatory obligations. Further, we may disclose, to the extent we deem such disclosure or transmission is necessary for satisfying the purposes set out above, to the following recipients:

- Other companies partnering with Optiniti such as the Software Provider(s). This data may be transferred in order to allow us to provide a full service to you, where other companies within perform components of the full service offering such as IT maintenance or support services;
- Any lawyers, external auditors or advisors, professional consultants, credit reference agencies, notaries, bailiffs, as well as any courts, regulatory, governmental, administrative or other official bodies as agreed or may be required by law, where such disclosure is necessary
 - (i) to comply with any applicable law or regulation;
 - (ii) to enforce applicable terms and conditions or policies;
 - (iii) to protect the security or integrity of our services; and
 - (iv) to protect our rights and interests;
- Third-party service providers or Data processor that provide IT services, identity verification checks, banking and payment processing services or other services to Optiniti, which are only authorised to process your personal data strictly for the purposes of providing these services and in accordance with our instructions. If applicable, we will enter with such third-party service providers into the relevant contractual agreements or the standard data protection clauses that would be required under the relevant data protection laws to ensure compliance with our instructions; and
- Third parties as part of mergers and acquisitions, provided that the prospective buyer or seller agrees to respect your personal data in a manner consistent with our Privacy Policy.

We will require any entity to whom we disclose your information or who may obtain it on our behalf to ensure its confidentiality, and to handle it in line with the legitimate purpose for which they are allowed to access it and in accordance with the applicable data protection laws.

We will not share or sell your information with third parties for their own independent marketing or business purposes without your consent.

Transferring Information Internationally

Personal data may be held at our offices and within third party agencies, service providers, representatives, auditors, lawyers and agents as described above. Some of these third parties may be based outside the EU and the European Economic Area (EEA).

Under data protection law, we may only transfer your personal data to a country or international organisation outside the EU/EEA where:

- the European Commission has decided the particular country or international organisation ensures an adequate level of protection of personal data (known as an 'adequacy decision');
- there are appropriate safeguards in place, together with enforceable rights and effective legal remedies for data subjects; or
- a specific exception applies under data protection law.

Adequacy decision

We may transfer your personal data to certain countries, on the basis of an adequacy decision. The list of countries that benefit from adequacy decisions will change from time to time. We will always seek to rely on an adequacy decision, where one exists.

Other countries we are likely to transfer personal data to do not have the benefit of an adequacy decision. This does not necessarily mean they provide poor protection for personal data, but we must look at alternative grounds for transferring the personal data, such as ensuring appropriate safeguards are in place or relying on an exception, as explained below.

It may be processed by staff working for us or for one of our suppliers, located outside the EU and / or the EEA. Such personnel may, for example, be involved in the execution of our support services. We will take all necessary steps to ensure that your personal data is treated securely and in accordance with this Privacy Policy and have adopted appropriate safeguards to protect it.

Transfers with appropriate safeguards

Where there is no adequacy decision, we may transfer your personal data to another country if we are satisfied the transfer complies with data protection law, appropriate safeguards are in place, and enforceable rights and effective legal remedies are available for you, as data subjects.

The safeguards will usually include using legally-approved standard data protection contract clauses. In this way, we make binding arrangements with such third parties so that your information is protected to the same standards as it is in the EU and EEA.

8. HOW LONG WILL YOUR DATA BE STORED?

We will process your personal data for the entire duration of the Collaboration Agreement your employer has concluded with us and for a period of ten (10) years after the termination of the Agreement to comply with the applicable anti-money laundering legislation and legal safe-keeping obligations. Further, any personal data will not be retained for longer than the time necessary for satisfying the purposes of its processing, subject to the general statutory limitation periods and the mentioned retention period where the applicable laws require that the personal data is retained for a certain period after the termination of our business relationship with you.

9. WHAT ARE YOUR RIGHTS REGARDING YOUR PERSONAL DATA PROCESSING?

You have the right to:

Right of access and communication of data

The Data subject has the right to access and consult the personal data that the company holds about him/her. The Data subject may also find out how the company obtained the data and to whom it was communicated. The Data subject may also request a copy of this personal data during processing.

In view of the company's obligation of security and confidentiality in the processing of personal data, the Data subject's request for access and consultation of the data will be processed subject to proof of identity, in particular by producing an electronic or paper copy (accompanied by a signature) of his or her identity card during the period of validity thereof. The request is, in any case, free of charge for the Data subject.

However, the company may object to requests that are manifestly abusive or unfounded (by their number or their repetitive or systematic nature, for example).

Right to rectify data

The European regulation allows the Data subject to request the rectification, updating or deletion of data concerning him or her which may be inaccurate, erroneous, incomplete or obsolete.

Right of opposition

The Data subject has the right to object to the processing of data in the following two situations:

- when the exercise of this right is based on legitimate grounds or

- when the exercise of this right aims to prevent the data collected from being used for commercial prospecting purposes.

Right to restrict

The Data subject may request the company to restrict the processing of his/her personal data in certain circumstances such as where he/she challenge the accuracy of the personal information, for a period of time to allow Optiniti to verify the accuracy of his/her personal data or in the event that he/she believe that the processing is unlawful. However, such an objection may not prevent us from storing his/her personal information.

Right to erasure

The Data subject has the right to request and obtain the deletion of data concerning him/her held by the company.

The company will comply with the Data subject's request if :

- the personal data are no longer necessary for the purposes for which they were collected;
- the processing of the data was based exclusively on the Data subject's consent and the Data subject withdraws his consent;
- the Data subject objects to the processing for well-founded reasons.

In any case, the request for erasure may be refused by the company if the request is necessary for the exercise or defence of legal rights or for compliance with a legal or contractual obligation on the part of the company.

Right to data portability

The Data subject may request that his or her personal data be transferred to a controller identical to the company. The Data subject may therefore request that the data be transmitted to the company in a structured, commonly used and computer-readable format.

How to exercise your rights

The aforementioned rights may be exercised by sending a letter to the company's address or by sending an e-mail to the following address: support@optiniti-group.com.

Response time

the company will respond to the Data subject's request in the same way as the Data subject exercised his right.

The company undertakes to respond to any request for access, rectification or opposition, deletion or any other additional request for information within a

reasonable time and in any event within a maximum of 1 month from receipt of your request.

Depending on the complexity of the request, the response time may be extended to 3 months, in accordance with the applicable European regulation.

10. HOW DO WE MANAGE AND PROTECT YOUR PERSONAL DATA?

We put a lot of effort and apply the highest technical and organisational standards ensuring that your personal data is secured and kept confidential. Any personal data that you provide to us is stored on secure servers, and we use rigorous procedures to protect against loss, misuse, unauthorised access, alteration, disclosure, or destruction of your personal data. We protect your personal information by maintaining physical, electronic, and procedural safeguards in compliance with the applicable laws and regulations. Part of the measures that we apply to provide a high level of security in terms of personal data management include, among others:

- Pseudonymisation – we process your personal data in such a manner that it can no longer be attributed to a specific person without the use of additional information which additional information is kept separately and is subject to specific technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person;
- Encryption – we apply cryptographic methods which convert certain information or data into a code to make it unreadable for unauthorized users;
- Minimisation – the personal data we demand from you is adequate, relevant and only limited to what is necessary in relation to the purposes for which such data is processed;
- Strict internal control on access to your personal data – access to your personal data is allowed only to those of our employees who need such verification to properly exercise their professional duties;
- Penetration testing – we perform regular scanning and penetration testing and services to identify potential security vulnerabilities and apply the relevant remedies to rectify them;

Ensuring ongoing application of integrity, confidentiality and education of all our employees.

We maintain security and incident response plans in the event of a physical or technical incident to handle this in a timely manner and limit any negative effect of such incident. Although we work hard to protect your personal data, we cannot guarantee that our safeguards will prevent every unauthorised attempt to access, use or disclose personal data.

Please recognise that you play a vital role in protecting your own personal data. When registering with our services, it is important to choose a password of sufficient length and complexity, to not reveal this password to any third parties, and immediately notify us if you become aware of any unauthorised access to/use of your account. If you believe that any of your account login details have been or might have been exposed, you can change your password at any time through our Website, as well as immediately contact our customer service. Given the nature of communications and information processing technology, we cannot guarantee that information, transmitted through the Internet, will be completely safe from intrusion by others.

11. CHANGES TO THIS PRIVACY POLICY

We may change this Privacy Policy from time to time by posting the updated version on our Website. Laws, regulations and industry standards evolve, which may make those changes necessary, or we may make changes to our business. We advise you to review this page regularly to stay informed and to make sure that you are happy with any changes. If the changes are significant, we will provide you with a more prominent notice such as an email notification or through the Services. If you disagree with the changes to this Privacy Policy, you should discontinue your use of our services. If we change this Privacy Policy in a way that will affect how we use your personal data, we will advise you of the choices you may have as a result of those changes.

12. PERSONAL DATA BREACHES

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. The Company is obliged to do this within 72 hours of becoming aware of the breach, where feasible following its framework for reporting and managing data security breaches affecting personal or sensitive data held by the Company.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, The Company is required to also inform those individuals/data subjects without undue delay.

The below procedures are there to provide a framework for reporting and managing data security breaches affecting personal or sensitive data held by the Company.

A personal data breach is defined as having the potential to affect the confidentiality, integrity or availability of personal data held by the Company in any format. Such breaches may happen for any number of reasons including:

- The disclosure of confidential data to unauthorised persons;
- Loss or theft of data and/or equipment on which data is stored;

- Inappropriate controls allowing for unauthorised use of information;
- Breaches in the Company's IT systems and security;
- Unauthorised access to computer systems e.g. hacking;
- Viruses or other security attacks;
- Breaches of physical security where data is kept;
- Leaving IT equipment unattended allowing unauthorised access;
- Emails containing personal data sent in error to the wrong recipient.

13. LEGAL DISCLAIMER

The Company may disclose your personally identifiable information as required by rules and regulations and when the Company believes that disclosure is necessary to protect our rights and/or to comply with any proceedings, court order, legal process served or pursuant to governmental, intergovernmental or other regulatory bodies.

The Company shall not be liable for misuse or loss of personal information or otherwise on the Company's website(s) that the Company does not have access to or control over. The Company will not be liable for unlawful or unauthorised use of your personal information due to misuse or misplacement of your passwords, negligent or malicious intervention and/or otherwise by you or due to your acts or omissions or a person authorized by you (whether that authorization is permitted by the terms of our legal relationship with you or not).

14. LEADING VERSION

This Policy can be translated into different languages. If there are any inconsistencies between different language versions, the English language version shall prevail.

Last updated: December 2023