PRIVACY POLICY

OPTINITI – 14/05/2024

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 / Platform[1]. 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 you 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;
    - verifying your identity, opening and managing your account on the Platform;
    - meeting our regulatory obligations;
    - processing your requests related to the Services;
    - managing client relationships by means of electronic, telephone or chat communication, entering into and executing transactions with financial instruments;
    - conducting a risk management control, data analysis and global supervision of your ongoing needs and enhancing the services offered to you;
    - improving and personalising our Services to enhance your experience;
    - 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: May 2024