Unilink

UNILINK END USER PRIVACY POLICY

Last updated: October, 24 2018

This document provides information about our an comprehensive affiliate management software Unilink, which being owned and developed by FinoTech Limited with a registered office at 5 The Mall street, London W5 2PJ (Incorporated under the Companies Act 2006 as a private company, registered in the Registrar of Companies for England and Wales, under the Company number: 10761117, TIN: 7311025296 - hereinafter referred to as: "***the Company***", "***We***", "***Us***", "***Our***") owns and develops tracking and digital advertising technology that enables advertisements (also called further ads) to appear within desktop and mobile websites, as well as within mobile applications. The aim of this document is to provide you transparent information how the Unilink runs and how the ***Data*** is processed, collected, and stored in the software.

The Company is committed to protecting the privacy of Internet users and fostering users' confidence in online advertising and marketing. Accordingly, we are committed to observing applicable industry guidelines and the General Data Protection Regulation ("***the GDPR***") enacted by the legislative body of European Union. ***The Company*** continues to evaluate enhanced ways to protect Internet users' privacy while seeking to deliver relevant advertising and custom online experiences to those users on behalf of our customers.

This document outlines ***Unilink End User Policy*** and provides you clear notice about the user's information we may collect and process online in connection with our services.

The Company's **Clients** use relevant technology to execute digital advertising campaigns and our tracking technology to monitor, analyze, and optimize the results of digital advertising campaigns. Such operations result in you having indirect (when advertisements are displayed within sites and apps) and direct (when you click any of those advertisements) interactions with our servers.

I. Glossary

1. ***Applicable Laws*** means any laws and regulations relevant to the collection, processing, and storage of personal data, especially all the personal data protection

laws and the General Data Protection Regulation (EU) 2016/679 (hereinafter referred to as " ***the GDPR***").

2. ***Ad Server*** means a server where advertisements are stored, managed, and delivered to ***You*** as a website end user. It might also provide a reporting module to check how the advertisements perform.
3. ***Cookie*** means a small text files stored locally by a website or ad server. By storing certain information in a cookie, those web browsers or ad servers are able to remember ***Your*** preferences and recognize websites visited and / or web browser used from one visit to another.
4. ***Client*** means the party, regardless of B2B or B2C nature, who submits an application (on the registration page: https://unilink.io/) and uses the Unlink software.
5. ***Domain Name*** means a character string that helps ***You*** to easily go to a website without the necessity of remembering IP addresses. A domain name must be unique for all domain names available on the Internet. It allows ***You*** to navigate to a website and discover an online advertisement.
6. ***Do Not Track (DNT)*** means an option of the web browser that sends a request to a web application to disable tracking of an individual user.
7. ***End User (Visitor)*** means a user of an Internet connected device, such as a visitor to a website or a user of an IoT device, or a visitor on an advertisement, landing page, or campaign.
8. ***Geographic Location*** means a piece of information where you are located based on an IP address. Precisely, this is a location of ***Your*** device that is connected to the Internet and based on that we are able to define a country, region, city, and ***Internet Service Provider Your*** device is connected to.
9. ***HTTP request header*** means the request header of HyperText Transfer Protocol. The HTTP protocol is used all around the world. Almost all content that shows up in the browser ***You*** see is transmitted to your computer (or other device connected to the Internet) over HTTP. For example, when ***You*** opened this policy in the browser, many HTTP requests have been sent. Each request contains an HTTP header in which there is information about the browser ***You*** use, the requested page, the server and much more.
10. ***HTTP request parameters*** means the request parameters of HyperText Transfer Protocol are additional pieces of information transmitted from one device to the other that ***You*** might see in the address bar of your browser. They are in the form of

name=value pairs separated from the URL by a *"?"*. There might be more than one name=value pair, where each of them are separated by an *"&"*.

11. ***IP Address*** means an Internet Protocol (IP) address is a set of numbers that each device has assigned to connect with other device over the Internet network. The IP address allows addressing and delivering the information to the right receiver. Every time a piece of information is sent, a device needs to communicate with other devices in a computer network to be able to deliver the message. Sending information in that context means every kind of activity such as surfing, exchanging emails, or downloading an application. The IP address is used to identify the device to which the message is supposed to be sent and find the best way to deliver it.
12. ***Legal Basis*** means the legal basis for the collection, processing and storage of ***Your Personal Data***
13. ***Personal Data*** or ***Data*** means any information relating to an identified or identifiable person as defined in article 4.1 of ***the GDPR*** i.e. any information relating to an identified or identifiable natural person ('***data subject***'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
14. ***Processing*** means any operation or set of operations which is performed upon ***Personal Data***, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction (for the purposes of this document, ***Process***, ***Processes*** and ***Processed*** shall have the same meaning).
15. ***Profiling*** means any form of automated processing of ***Personal Data*** consisting of the use of ***Personal Data*** to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
16. ***Referrer Domain*** means the address of a website that led someone, as a visitor, to another page.
17. ***Retargeting*** means a strategy of online targeted advertising when information is gathered to address ***Visitor's*** preferences based on their previous actions / choices.

18. ***Request Time*** means the time when a query to the Unilink database is sent. Every time when someone clicks an advertisement, the query request is made, so the Unilink is able to store the information about the visit.
19. ***User Agent*** means information about a device, operating system, web browser is being used to access a website.
20. ***You, Your, Yours (Visitor, Visitors, Visitor's, Visitors')*** means a person who can visit digital advertising campaigns on the Internet.

II. What is Unilink?

Unilink is a cloud-hosted analytics solution, designed for combining all your affiliate programmes and monitor them in one place, implementing various account settlement methods for different groups of your affiliates. In other words, the Unilink platform enables ***Clients*** to make their online campaigns more efficient and profitable by analyzing the ad-related data and then, optimizing the campaign by addressing them in the most effective way. Therefore, ***Clients*** can set transparent rules and supervise the performance of their affiliates and track the traffic and effects of their campaign, knowing which affiliates get best results by means of reach, clicks and conversions. There are provided the detailed cloud-base solutions, aimed at upload and manage media like landing pages, widgets, display ads, referral links and more. Moreover Unilink make sure that ***Client's*** affiliates use the media quality wanted and checked by ***Client***, which ads perform best.

Unilink collects data about different activities of online visitors to allow its ***Clients*** to address ads to the right audience and display more relevant advertisements on websites. Those ***Visitors*** are Internet users who surf through the websites, send emails, communicate on social media and see those ads appearing in the content. To display the advertisement at the right time and in the right context, Unilink processes the collected ***Data*** to measure the ad effectiveness and coverage. All kinds of data are gathered for statistical and reporting purposes and processed collectively as records of certain information to produce a meaningful approach while running an online campaign.

III. Unilink role in Personal Data Processing

While ***Clients*** use Unilink relevant technology to execute digital advertising campaigns and our tracking technology to monitor, analyze, and optimize the results of digital advertising

campaigns, ***the Data Controller*** of ***End User's Personal Data*** is ***the Company***. In the other situations concerning using of Unilink software ***the Company*** is ***the Processor*** of its ***Clients***, which means that ***the Company*** is ***Processing the Personal Data*** solely on behalf of and based on ***the Client's*** instructions.

IV. What kind of Personal Data does Unilink collect and for what purposes?

In order to perform services related to Unilink software, ***the Company*** is intended on collecting and processing certain information about ***You*** and ***Your*** device. Some of this information (including, for example, your IP addresses and certain unique device identifiers) in conjunction with other ***Data*** provided by ***You*** may be identified a particular computer or device and be considered as ***Personal Data*** in some jurisdictions, including the European Union. This kind of ***Data*** enables us to provide aggregated reporting and analysis of the performance of ***Client's*** advertising campaigns.

The Unilink platform does not collect any ***Data*** which by itself identifies an individual such as a name, address, phone number, email address.

The Company also do not collect any "sensitive" or "special categories of ***Personal Data***" as defined under the European data protection laws as well as ***Personal Data*** of children.

IP Address

An ***IP Address*** is used to identify the device's location as well as, to some extent, user's location. Based on the ***IP Address visitor's*** country, region, city can be characterized and stored in the Unilink software. Moreover, some more technical specifications are processed such as ***Internet Service Provider*** or mobile carrier and what type of the connection ***You*** use. This data is stored to adjust the online advertisements that are displayed on websites and identify automatic computer programs that might affect ***Client's'*** reporting. Additionally, the ***IP Address*** is used to limit the number of times a visitor is exposed to a single advertisement.

User Agent

A ***User Agen***t helps Unilink to identify what kind of a device a visitor uses (TV, desktop, tablet) and which model it is. Even more, this piece of information is stored to establish

device's parameters such as browser and browser version, operating system, and operating system version. It also allows Unilink to detect the automatic computer programs and fraud attempts. What is more, the user agent is used to limit the number of times a visitor is exposed to a single advertisement.

HTTP Request Header

Information from HTTP request headers is used to determine a ***Visitor's*** language and referrer domain. That data is then used to present an appropriate advertisement to the end user. It is also stored for analytical purposes.

HTTP Request Parameters

The HTTP request parameters are used to transfer information from third-party services to the Unilink and the other way round. Based on that, the Unilink ***Clients*** are able to find target audiences more effectively and message through appropriate channels. It is also stored for analytical purposes.

Device ID

A ***Device ID*** is a unique identifier used to accurately measure actions taken by a specific device. It plays a role in personalization, distribution, and performance of the traffic sent to a visitor. The ***ID*** enables us to do cross-device matching meaning that the advertisement will be displayed only on one device that belongs to a particular user. It means that if ***You*** are an owner of more than one devices connected to the Internet, the ***IDs*** of those devices can help us to identify ***You***, determine which advertisement was displayed on which device, and eliminate ad display repetitions for ***You***.

Request Time

This is an exact date and time of interaction with Unilink servers. It is used to present an appropriate advertisement to the ***End User***. It is also stored for analytical purposes.

Unique Identifier (UID)

A unique identifier generated by the software enables us to match registered events and control the frequency of those events in Unilink. Notably, the publisher partners may share with us additional demographic information, such as age or gender, in order to enable more

accurate targeting. Although, ***the Company*** does not use this information to maintain any kind of persistent user's profile database.

V. How does Unilink collect Personal Data?

The Unilink uses ***Cookies***, and in some cases non-cookie technologies, to collect ***Data*** associated with particular web browsers or devices that you, as a ***Visitor***, use.

Unilink uses both types of ***Cookies***: ***Session Cookies*** and ***Persistent Cookies***. Those ***Cookies*** are used not only to follow ***Visitor's*** activities, but also to improve ***Visitor*** experience while surfing through the Internet websites. ***Session Cookies*** does not remain after closing a web browser and does not store any information afterward. Persistent cookies are stored locally on ***Your*** device and may be used by ***Your*** web browser on subsequent visits to any website. They are used to remember your preferences and personalize the ad content.

In the tracking part of the advertising platform, Unilink also uses non-cookie technology such as pixels to set up the communication between your web browser and a server.

Tracking

In the tracking part of the Unilink or the external providers (e.g. Amazon Web Services - "AWS") the following technology may be used to gather ***the Data***:

- ➔ ***Impression Cookie***. Some of ***Clients*** are only interested in displaying advertisements on websites, so the ads might be noticed by an ***End User***. This type of advertising refers to impressions or ad views. ***The Cookie*** helps us to monitor this type of activities. It is ***a Session Cookie***, so it exists as long as ***Your*** session lasts in ***Your*** web browser.
- ➔ ***Conversion Cookie***. This is ***a Cookie*** that allows to combine a display of an advertisement with a ***Visitor's*** actions that happen for a particular offer afterwards. ***Clients*** may define what kind of an action the ***Visitor*** should take upon to call the ad display successful. This ***Cookie*** allows Unilink to define, whether the action happened or not for a particular ***Visitor***. That record allows us to measure ***Visitor's*** behavior and personalize the ads displayed on websites. It expires after 30 days.
- ➔ ***Lander Cookie.*** This is ***a Cookie*** associated with a visit on a displayed advertisement. It stores different pieces of information about the visit itself as well as

other parameters such as a web browser type, web browser version, device ID. This data is only used for statistical and reporting purposes in AWS systems. It expires after one day.

- ➔ ***Unique Session Cookie.*** It is used to detect whether a visit is the first visit of a ***Visitor*** for a particular advertisement or not. It is ***a Session Cookie***, so it exists as long as your session lasts in your web browser.
- ➔ **Tracking Pixel:** This is an invisible, very small (1 x 1) pixel tag that ***Client*** can put on a website. When ***You*** as a ***Visitor*** open a website where the tracking pixel is placed, the information is sent to Unilink. Pixel tags are used in combination with ***Cookies*** to track user's activities while surfing through websites by a particular browser on a particular device.

In the digital advertising, the ***Data*** is collected using the following cookies:

- ➢ ***Sync cookie***. This is a unique number that will be assigned to you as a ***Visitor*** when an advertisement shows up in a website for the first time. ***The Cookie*** stores the data to inform us that ***You*** have seen a certain set of advertisements before, so ***We*** may vary them not to overload ***You*** with the same content all the time. Shortly, it enhances the advertisement selection. It expires after 30 days.

VI. For what purposes Unilink use End User data?

The Data collected and stored in the Unilink is used to increase the ad relevance and adjust the ad display to the changing needs of the ad ***Visitor***. Particularly, the data is used by Unilink for:

1. ***Cross-device matching*** - to identify to how many devices a visitor is associated with to cut off ad display repetitions.
2. **Fraud detection** - to monitor the quality of traffic for ***Clients*** and blacklist those sources that generate fake visits / clicks.
3. ***Frequency capping*** - to limit the number of times a ***Visitor*** is exposed to a single advertisement.
4. ***Profiling*** - to evaluate of certain personal aspects relating to a natural person for ensuring ad security and ad fraud functionality, in particular to analyse or predict aspects concerning that natural person's personal preferences, interests, behaviour, location and usage of ***Cookies*** technology in connection with an ***End User's*** device.

5. ***Remunerating*** - to calculate of remuneration, based on e.g. number of conversions or other factors, mutually agreed between ***the Company*** and ***the Client***.
6. ***Reporting, analysis, and optimization*** - to measure the effectiveness of online ad campaigns what helps to address the advertisements to right audiences and based on the collected data improve the performance of the campaigns. Briefly, to determine how visitors respond to advertisements they see on the Internet.
7. ***Retargeting*** - to allow ***the Clients*** to address ***Visitor's*** preferences based on their previous actions / choices.

VII. Legal Basis for Processing User Information

If ***You*** are a European Union End user or ***the GDPR*** applies to you under the ***Applicable Law***, ***the Legal Basis*** for collecting and using the ***End User's Data*** described above will depend on the ***User's Information*** concerned and the specific context in which ***We*** collect it.

The Company declares that it relies mostly on contractual ***Legal Basis*** for ***Personal Data Processing*** i.e. ***Processing*** is necessary for the performance of a contract to which ***the Client*** is party [**Article 6(1b) of the GDPR**] when ***Your Personal Data*** is processed in order to deliver ***End Users*** targeted advertising and use ***Cookies*** technology in connection with an ***End User's*** device. ***The Company*** relies solely on consent to collect [**Article 6(1a) of the GDPR**] and / or process end ***User's Information*** in case of subscription of the newsletter from **Our** blog, where such consent will be obtained in compliance with applicable laws.

We may also use the end user's personal data because of our legitimate interests [**Article 6(1f) of the GDPR**] to:

a. Operate and improve our technology
b. Enable standard advertising controls
c. Prepare reports that summarize ***Visitor's*** activity
d. Analyze and report on the advertisement's performance (such as tracking views of ad as well as click-through rates on ads), campaign reporting, and campaign forecasting
e. Protect, investigate, and deter against fraudulent, unauthorized, or illegal activity.
f. Determination, prosecution of claims and enforcement of claims.

Balance of interests. After assessment ***the Company's*** interests and ***Your*** interests, rights and freedoms, ***the Company*** believes that statistical, analysis and protection measures on the use of particular Unilink functionalities and facilitating the use of the Unilink as well as ensuring the IT security of the services related to Unilink will not interfere excessively with ***End User's*** privacy or will not constitute an excessive burdensomeness for ***End User***. In the course of evaluating ***End User's*** interests, rights and freedoms, ***the Company*** has taken into account the following circumstances: ***the Company*** does not process ***the Personal Data***, based on which end users could be exclusively identified; upgrading the standards of services provided by ***the Company***, resulting in the securing of ***End User's Personal Data*** as well devices, which are being used during contact with ***the Company***; avoiding the risk of suspension of the Unilink due to the illegal activities of dishonest Unilink ***Users***; preventing ***the Company*** from malicious actors.

VIII. How long does Unilink store Personal Data?

The collected data is stored using generally accepted security standards. ***The Data*** retention in the Unilink is from the day of the account registration till the closure of account after termination of the cooperation between ***the Client*** and ***the Company***. This data is used for reporting and analysis. When a ***Client*** removes their data from Unilink, their storage and retention of data is governed by ***the Privacy Policy*** and applicable regulations. The process of removing the collected data from Unilink might take up to 1 month.

IX. Your Choices and the Opt-Out Option

The opt-out option is applicable for ***End Users*** who see an online advertisement set by a ***Client***. ***Visitors*** of advertisements that are a part of digital advertising may choose either the opt-out or Do Not Track option.

If ***You*** wish to opt out of being tracked with desktop and mobile website environments from Unilink, ***You*** should use the opt-out option. Unilink only ***Processes the Data*** collected by its ***Clients*** meaning that the Unilink ***Clients*** are obliged to deliver the opt-out option and make it accessible to ***You*** as a ***Visitor*** to an online advertisement. Unilink makes every effort to support its ***Clients*** to provide such a solution for ***You***, thus ***You*** can find below procedures how to make a request to opt out of being tracked.

The Opt-Out Option for Tracking Advertising (Tracking)

Due to the fact, that domain name is set for each ***Client*** individually, ***You*** need to get in touch with ***the Client*** of the online advertisement to find out the correct ***Domain Name*** under which the online advertisement is set. Once the Unilink ***Client*** replies with ***the Domain Name***, ***You*** can provide the link in an address bar in your web browser to be able to opt out.

Opting out of being tracked with desktop and mobile website environments from the tracking advertising part of Unilink is valid for at least 30 days for a web browser where the opt-out option has been set. The option can be enabled only for a particular web browser meaning that if ***You*** switch to other web browsers, clear cookies, or use a browser's incognito mode, ***You*** need to go through the opt-out procedure once more. When the opt-out option expires, ***You*** need to repeat the same procedure to turn it on again.

The Opt-Out Option for Digital Advertising

Desktop Website Environments

If ***You*** wish to opt out of being tracked with desktop website environments, follow the steps:

(*Google Chrome web browser, version 66.0.3359.139, official build*)

From ***Your*** web browser, select Menu (3 bars at top right of window).
Select Settings and then scroll down to Advanced. Expand the Advanced section.
In Privacy and security, select Content Settings > Cookies.
Turn on the Block third-party cookies toggle.

(Safari web browser, version 11.1 (13605.1.33.1.4))

From the main menu in ***Your*** web browser, select Safari > Preferences.
Go to Privacy and then select the Block all cookies checkbox.
Confirm ***Your*** choice by clicking the Block All button.
Mobile Website Environments

Opting out of being tracked with desktop and mobile website environments from the digital advertising part of Unilink is valid for indefinite period of time till another save ***Your*** data for a web browser where the opt-out option has been set. The option can be enabled only for a particular web browser meaning that if ***You*** switch to start using other web browser, ***You***

need to go through the opt-out procedure once more. When the opt-out option expires, ***You*** need to repeat the same procedure to turn it on again.

The Do Not Track Option

If ***You*** wish to opt out of being tracked with desktop and mobile website environments from the digital advertising part of Unilink (Unilink ***DSP***), ***You*** may use the Do Not Track option. This option does not work for the tracking part of Unilink.

Desktop Website Environments

If ***You*** wish to turn on the Do Not Track option in ***Your*** web browser for you desktop website environment, follow the steps:

(*Google Chrome web browser, version 66.0.3359.139, official build*)

From ***Your*** web browser, select Menu (3 bars at top right of window).
Select Settings and then scroll down to Advanced. Expand the Advanced section.
In Privacy and security, find Send a “Do Not Track” request with ***Your*** browsing traffic. Turn on the toggle.
Click Confirm to activate the Do Not Track option in ***Your*** web browser.

(*Safari web browser, version 11.1 (13605.1.33.1.4)*)

From the main menu in ***Your*** web browser, select Safari > Preferences.
Select Privacy and then Ask websites not to track me.
Mobile Website Environments

X. European Data Subject Rights

If ***You*** are a European Union end user or ***the GDPR*** applies to ***You*** under ***the Applicable Laws***, ***You*** have certain rights and protections under the law regarding the collection, processing, and use of information about ***You***.

The Company ensures the implementation of ***Your*** rights listed below. ***You*** can exercise ***Your*** rights by submitting a request via email.

The right to withdraw consent.

You have the right to withdraw any consent, if the processing of ***Your Personal Data*** on Unilink is solely based on ***Your*** consent and ***You*** provided it at the time of registration to Unilink, as well during using individual functionalities offered on Unilink - only in event of Unilink as well individual services and functionalities offered on Unilink provide ***Data Processing*** based on ***Your*** consent. Withdrawal of consent has effect since the moment of its withdrawal. The withdrawal of consent shall not affect the lawfulness of processing, performed by ***the Company*** based on ***Your*** consent before its withdrawal.

Withdrawal of consent does not entail any negative consequences for ***You***. However, it may prevent ***You*** from continuing to use the Unilink or functionality that ***the Company*** can lawfully provide only based on ***Your*** consent.

Legal basis: Article 7(3) of the GDPR.

The right to object to the Data being used

You have the right to object at any time to the use of ***Your*** personal data, if ***the Company*** processes ***Your Data*** based on its legitimate interest, e.g. in relation to the improving of Unilink services.

If ***Your*** objection turns out to be legitimate and ***the Company*** has no other ***Legal Basis*** to ***Process Your Personal Data***, ***the Company*** will delete ***Your*** data which is subject of the objection raised by ***You***.

Legal basis: Article 21 of the GDPR.

Right to erasure (‘right to be forgotten’)

You have the right to request the erasure of all or some of ***Your Personal Data***.

You have the right to request erasure of ***Personal Data*** if:

a) ***You*** withdrew ***Your*** specific consent to the extent to which ***Your Personal Data*** was processed based on ***Your*** consent;

b) ***Your Personal Data*** has ceased to be necessary for the purposes for which it was collected or processed;

c) ***You*** raised an objection to the use of ***Your*** data for marketing purposes;

d) ***You*** raised an objection to the use of ***Your*** data in order to conduct statistics on the use of Unilink, and the opposition was considered justified;

e) ***Your Personal Data*** is ***Processed*** unlawfully.

Despite the request to erase ***Personal Data***, in connection with opposition or withdrawal of consent, ***the Company*** may retain certain ***Personal Data*** provided by ***You*** in the field of asserting or defending claims. This applies in particular to ***Personal Data***, received solely from ***You***, regardless of means of communication, without limitation: name, surname, email address, documents provided by ***You*** during e.g. the email communication with ***the Company***, which ***the Company*** retains for purposes of handling complaints and claims related to the use of Unilink.

Legal basis: Article 17 of the GDPR.

Right to restriction of Processing

You have the right to request a restriction on the ***processing*** of ***Your Personal Data***. If ***You*** submit such a request, it will prevent ***You*** from using certain functionalities or services, involving the ***Personal Data*** processing covered by the request. ***You*** will also not receive any messages, including marketing messages.

You have the right to request restrictions on the use of ***Your Personal Data*** in the following cases:

a) when ***You*** contest the accuracy of ***Your Personal Data*** - then ***the Company*** will restrict their use for the time needed to verify the accuracy of ***Your Data***, but no longer than for 7 days since the receipt of ***Your*** request;

b) if the ***Processing*** of ***Your Data*** is unlawfully, and instead of erasure ***Your Personal Data***, ***You*** will demand restriction of their use;

c) where ***Your Personal Data*** has ceased to be necessary for the purposes for which ***the Company*** has collected or used it, but it is necessary for ***You*** to determine, assert or defend claims;

d) if ***You*** object to the use of ***Your Data*** - then the restriction occurs for the time needed to consider whether, due to ***Your*** special situation, protection of ***Your*** interests, rights and freedoms override the interests based on which ***the Company*** processes ***Your Personal Data.***

Legal basis: Article 18 of the GDPR.

Right of access to the Data.

You have the right to obtain confirmation from ***the Company***, whether ***the Company*** process ***Your Personal Data***, and if this is the case, ***You*** have the right to:

a) get access to ***Your Personal Data***;

b) obtain information about the purposes of processing, categories of ***Personal Data*** being processed, the recipients or categories of recipients of this ***Data***, the planned period of storage of ***Your Data*** or criteria for determining this period, information concerning ***Your*** rights under ***the GDPR*** and the right to file a complaint to the supervisory authority, the source of these ***Data***, on automated decision-making, including profiling and safeguards applied in connection with the transfer of these data outside the European Union;

c) obtain a copy of ***Your Personal Data***.

Legal basis: Article 15 of the GDPR.

The right to rectify Your Personal Data

You have the right to rectify and supplement ***Your Personal Data***. ***You*** have the right to request us to correct this ***Data*** (if it is incorrect) and to supplement it (if it is incomplete).

Legal basis: Article 16 of the GDPR.

The right to Data portability.

You have the right to receive ***Your Personal Data*** that ***You*** provided to ***the Company*** and then send it to another ***Personal Data Controller*** chosen by ***You***, e.g. to another ***Controller*** of similar services. ***You*** also have the right to request that ***Personal Data*** be sent by ***the Company*** directly to such other controller, if it is technically possible.

The Company will send your ***Personal Data*** in the form of a csv file. The csv format is a commonly used, machine-readable format that allows you to send the received ***Data*** to another ***Controller*** of ***Personal Data***.

Legal basis: Article 20 of the GDPR.

When does the Company meet Your request?

While - by exercising the aforementioned rights - ***You*** request, that ***the Company*** comply with this request or refuse to comply with it without delay, but no later than one month after receipt. However, if - due to the complexity of the request or the number of requests - ***the Company*** will not be able to meet ***Your*** request within a month, ***the Company*** will meet them within the next two months, informing ***You*** in advance about the intended extension.

For technical reasons, ***the Company*** always needs 72 hours to update the settings ***You*** have selected in ***the Company's*** systems. Therefore, it may happen that ***You*** will receive an email from ***the Company*** during the system update, from which ***You*** have given up.

If ***You*** would like to exercise any of these rights, please contact ***Us***: dataprotection@finotech.com. Please include information that will enable ***Us*** to verify ***Your*** identity within ***Your*** request.

Filing complaints, inquiries and applications

You can make complaints, requests and applications to ***the Company*** regarding the processing of ***Your Personal Data*** and the exercise of ***Your*** rights.

If ***You*** believe that ***Your*** right to the protection of ***Personal Data*** or other rights granted to ***You*** by virtue of ***the GDPR*** have been violated, ***You*** have the right to fill a complaint against ***the Company*** to the Information Commissioner's Office .

XI. Information Transferred from Third-Party Services

This document does apply only to usage of the ***Data*** by Unilink and does not explain the practices of other third-party advertisers or advertising networks. ***The Company*** does not control the privacy practices of such third parties, and ***You*** are obliged to get familiar with the privacy policies of those third parties when ***You*** use their services.

XII. Transfer of Personal Data Outside EEA

The Company cooperates with customers and partners throughout the world, including in the European Economic Area (EEA) as well as countries outside of the European Economic Area (EEA).

In order to ensure that ***Your Personal Data*** is adequately protected when transferred outside of the EEA, ***the Company*** relies on EU-U.S. Privacy Shield Program – Privacy Shield is a “partial” adequacy decision, as, in the absence of a general data protection law in the U.S., only the companies committing to abiding by the binding Privacy Shield principles benefit from easier ***Data*** transfer. In such cases ***Your Personal Data*** will be transferred to the territory of USA in accordance with applicable laws, with appropriate safeguards in place, only to Privacy Shield certified vendors (according to the EU Commission Decision 2016/1250) or by using standard contractual clauses adopted by the European Commission (EU Commission Decision on standard contractual clauses for the transfer of ***Personal Data*** to processors established in third countries under Directive 95/46/EC (the “Model Contract

Clauses"), or based on other applicable transborder data transfer mechanisms, or has entered into inter-company EU "model clause" agreements.

You may contact us if ***You*** require a copy of the safeguards which ***We*** have put in place to protect ***Your Data*** transferred outside of the EEA and ***Your*** privacy rights in these circumstances.

You may also learn more about:

Privacy Shield Program here:
https://www.privacyshield.gov/Program-Overview

and here:

https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-privacy-shield_en.

EU Commission Decision on standard contractual clauses for the transfer of ***Personal Data*** to processors established in third countries here:

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32010D0087

and here:

https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en

XIII. Security

The Company uses various security technologies and procedures that help protect ***Your Personal Data*** from unauthorized access, use, disclosure, alteration, or destruction.

The Company uses encryption in the transmission of ***Your Personal Data*** between ***Your*** system and ***Company's***, and ***the Company*** uses firewalls to help prevent unauthorised persons from gaining access to ***Your Personal Data***. All supplied sensitive / credit information is transmitted via Secure Socket Layer (SSL) technology.

The Company maintains physical, electronic, and procedural safeguards in connection with the collection, storage, and disclosure of ***Your Data***. ***The Company*** security procedures mean that we may request proof of ***Your*** identity before we disclose ***Personal Data*** to ***You***.

The Company relies only on vendors who ensure an appropriate level of security of ***Your*** data. In this context, ***the Company*** uses only secure cloud servers, including AWS cloud – a secure, private cloud platform. AWS participates in the EU-US Privacy Shield framework. Amazon Web Services is the Company's (sub-)processor. AWS Amazon cloud platform uses various security technologies and procedures to protect personal data and is compliant with third-party assurance frameworks such as without limitation: ISO 27017 for cloud security, ISO 27018 for cloud privacy, PCI DSS Level 1, and SOC 1, SOC 2, and SOC 3. For more details please see AWS Amazon security and privacy policy at www.aws.amazon.com.

XIV. Retention of the Data

The Company stores ***Your Data*** for a period of time required for the purposes for which it was collected using generally accepted security standards and in compliance with applicable laws. ***The Company*** will not retain ***Your Personal Data*** for longer than 2 years since the date of its collection.

XV. Children

Protecting children's privacy is very important to ***the Company***. Our software is not intended for, designed to be used by, or targeted at children. ***The Company*** does not allow its ***Partners*** and ***Clients*** to send to it ***Personal Data*** of children as defined under ***the GDPR***.