This Policy regulates the processing of personal data collected from visitors and / or users through the site www.lpin.ro, but also through our social network accounts (Facebook, Linkedin, etc.).

The operator of personal data is the Swimming Performance League Association, based in Corbeanca Commune, 32E Hipodromului Street, Ilfov County, Romania, with CUI: 40045613 (hereinafter referred to as the operator, LPIN, us or ours).

The person in charge of personal data protection can be contacted at the following contact details: e-mail: contact@lpin.ro.

The processing of personal data of individuals is mainly regulated in EU Regulation no. 679/2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC (GDPR) - the official text can be consulted at https: // eur-lex .europa.eu.

The terms used in this Policy have the meaning defined in the GDPR.

I. CATEGORIES OF PERSONAL DATA AIMED. THE SOURCE FROM WHICH IT COMES FROM. OBLIGATION OF SUPPLY (if applicable)

According to the Terms and Conditions, you must be at least 18 years old in order to use the Platform. Therefore, we do not want to collect or process data from people under the age of 18. We also do not collect or process sensitive data provided by GDPR and please do not send us such data through the contact form, e-mail, messages or in any other way.

Types of data processed:

• profile data, such as: name, surname, e-mail, password; optional: phone, photo (when logging in via Facebook), gender, country.

We receive this data from the user when they create the account by choosing the New Account option or when modifying or adding additional profile data. The password is encrypted, we do not have access to it.

The user must provide us with this data (except the optional ones) in order to create the account and use the services offered by LPIN. Without providing this data, the user will not be able to use the services offered by the Platform.

Optional data enhances the user experience; they are not mandatory.

This data can be changed at any time in the account settings.

• account data, such as: billing data, account opening date / account changes, user-expressed options.

We receive some of this data from the user when the account is created or when the account data is modified or supplemented. The rest of the data is generated by the Platform as we use the services offered.

Billing data is required to generate the invoice for services or products purchased through the Platform. In their absence, the invoice is issued in the name of the user. The invoice is communicated to the e-mail address registered in the user account.

• bank card data: we process this data in a limited way as follows:

The user registers the bank card data directly in the secure, independent platform, offered by the payment services processor we collaborate with, respectively by NETOPIA FINANCIAL SERVICES S.R.L., registered at the Trade Register under no. J40 / 12763/2020, unique registration code RO43131360, headquartered in Dimitrie Pompeiu Boulevard 9-9A, Building 24, 4th floor, Bucharest 020335.

It is PCI DSS (Payment Card Industry - Data Security Standard) mandatory certification for storing and viewing sensitive card information).

The data required by the payment processor we work with includes, as a rule: card number and holder, card expiration date and CVC / CVV2 code.

The payment service provider independently processes the data you enter into its secure platform. Details on how the secure platform processes this data can be found at: https://netopia-payments.com/politica-de-confidentialitate/.

We receive from the payment processor, in order to verify the payment: the last four digits of the bank card number, its expiration date, card status data (stolen, expired, etc.) and the name of the card issuing processing company (eg Visa / MasterCard).

This data is filled in automatically in the user account of the Platform.

• data on payments, such as: payments made, (possibly) data on the lack of cash on the bank card associated with the account, data on the status of payments, data on the status of the card (stolen, expired, etc.).

This data is collected from the secure payment processor platform.

• data from communications, such as: site contact form, chat, Facebook / Linkedin messaging, notifications / complaints, requests for support, various requests, communications sent by users, ratings, recommendations received from users. Such communications may contain various data cu personal, such as: name, address, e-mail, telephone, message data.

We receive this data when we are sent messages through the contact form or through the chat on the site www.lpin.ro, through Facebook or Linkedin messaging or when we are sent various requests or other communications, in writing or by phone to any of our contact details (including call center).

The transmission of identification data (name) and contact details (address, e-mail, telephone) are necessary in order to be able to register the request, to make the necessary checks, to respond to communications (as appropriate) and, in some cases, to could identify the person. Without them, we may not be able to respond properly to the request. In the contact form, the transmission of the telephone number is optional.

When you contact us via Facebook / Linkedin messaging, we may view data that is public on your profile on that social network (e.g., name, contact information, profile picture, etc.). From these data we can use, as appropriate, name and surname, contact details, to respond to the request.

Keep in mind that these social networks in turn process the content of messages transmitted through these means. Please read carefully the Data Use Policy specific to these networks, namely Facebook

(https://www.facebook.com/privacy/explanation) and Linkedin (https://www.linkedin.com/legal/privacy-policy) before contacting us through the specific messaging of these social networks.

Also, depending on the type of communication, the provision of certain data by you may even be a legal obligation.

• data on the use and operation of the Platform, such as: cases where the Platform or other systems (eg Internet) do not work properly, the date and time you access the Platform, the type of browser used and related information (such as browser settings) , the pages viewed on the Platform and the duration of the viewing, sites or services of third parties that you have used before interacting with our services.

We collect this data when you use the Platform, including through cookies or other similar means.

• cookies and similar technologies: on the website we can store and collect information through cookies and similar technologies.

Details about these technologies, how we use this information and how you can block or delete cookies can be found in the Cookies Policy.

Data update

It is very important that the data we process about you is accurate and correct. Please periodically check your account data and change this data if you notice any errors or changes. We will periodically send you notifications to remind you to update your data.

II. PURPOSE AND LEGAL BASIS OF THE PROCESSING

We will use your personal data for the following purposes:

2.1 Offering and providing to the user the services offered by the Platform

We use the data collected in order to offer and subsequently provide the services we provide to you through the Platform, in compliance with the contractual conditions. Thus, we use the data for purposes such as:

• creating, updating and managing the user account

• identity verification

• payment of the contribution for participation in competitions, invoicing of contributions

• transmission of invoices and collection of tariffs

• transmission of various information regarding the services used through the Platform and the status of the related payment, by e-mail or telephone

• blocking the use of services in case of unpaid services

• resolving any issues related to the use of the Platform, such as related to the services used, related payments, the operation of the Platform, etc.

• closing the user account

• providing support services, including providing answers to requests or questions regarding the services provided through the Platform

• carrying out internal technical operations necessary for the provision of services, such as monitoring and analysis of the operation and use of the Platform, function tests, interventions and service in case of operational problems

The processing of data for the purposes mentioned above is, in most cases, necessary for the conclusion and performance of the contract between you and us. Also, certain processing subject to these purposes is imposed by our obligations under the law, including tax, accounting, archiving legislation.

We base the processing of data and optional data (such as phone, gender, photo) on your prior consent. Sending notifications over the phone is also based on your prior consent. You are not obliged to give us this consent! You can use the services offered by the Platform even if you do not agree to process this data. Details on how you can express or withdraw your consent and on the consequences of the withdrawal found in Section V below.

Lack of consent may either affect the operation of the services, or the user experience will be less pleasant (for example, you will no longer receive notifications on the phone about the services used).

2.2 Customer support

We use personal data received through the contact form, through chat, Facebook / Linkedin messaging, collected by telephone (including call center), received at contact e-mail addresses or through any other forms of communications / notifications / petitions, for you assist in connection with matters for which you contact us, assistance which may include, as appropriate:

• analysis and solution of formulated issues

• transmission and investigation of the reported issues to / by the responsible persons

• sending a response to the contact details provided

• monitoring and analyzing the customer support activity in order to improve the services offered.

We base these processing either on the need to take steps at the request of the data subject to conclude a contract, or on our legitimate interest to carry out our activity in the best conditions, providing support to users, as well as to develop commercial activity, ensuring that all the measures we take guarantee a balance between our interests and your fundamental rights and freedoms.

Depending on the specific situation, certain processing may be imposed by our obligations under the law, such as the obligation to respond to requests for personal data.

2.3 Marketing activities

We want to be able to periodically send you Marketing Information (commercial communications) about the new services we offer through the Platform, but also about promotions or other offers that may interest you. Thus, we can send you various messages, by e-mail or SMS, including in the form of a newsletter, containing information about services similar or complementary to those you have used, completely new services compared to those used, offers or promotions, such as and other business communications related to our business, such as market research and opinion polls.

We rely on the transmission of Marketing Information with your prior consent. You are not obliged to give us this consent!

You may use the services provided by the Platform even if you do not agree to send us such Marketing Information. Details on how you can express or withdraw your consent and the consequences of the withdrawal can be found in Section V below.

2.4 Safety and security

We use some of the data collected to ensure and maintain the security and integrity of the Platform and your user data. Thus, we use the data collected on, for example, the device used, profile data or other information for:

• prevent and detect fraud, theft / loss / deletion of data, unauthorized access and / or use, inappropriate behavior and the like on the Platform, devices, computer systems and networks, software, databases, servers, e-mails, and in general on the goods and means used by ParkPay to provide the services through the Platform

• limit or eliminate their effects

• analyze, summarize and, where appropriate, report such incidents to the competent authorities.

In some cases, such incidents may block your use of the Platform.

We base such processing mainly on our legitimate interest in conducting our business in the best possible conditions and in protecting our business and business interests, including those conducted through the Platform, ensuring that all measures we take We guarantee a balance between our interests and your fundamental rights and freedoms.

Depending on the specific situation, we may rely on the processing of data for this purpose, to the extent necessary, including in the legitimate interest of others, when fraud may affect the data of users or other parties (eg service providers), or various legal obligations such as the obligation to report theft, fraud or security incidents to the authorities or to take other measures to prevent or detect fraud.

2.5 Analysis and improvement of services provided

We want to offer you the best experience of using the Platform and the services offered through it. For this, we may collect and use certain information, in particular in connection with the way users use the Platform, in order to analyze the operation of the Platform, its improvement and the services provided, in order to develop new functions. nalities.

We base these activities on our legitimate interest in carrying out and developing our business activities, always taking care that your fundamental rights and freedoms are not affected.

In the case of cookies and similar means used on our site, we base our processing on your prior consent (except for cookies that are strictly necessary for the operation of the site). Details on how you can express your consent or block or delete cookies can be found in the Cookies Policy.

Lack of consent may either affect the operation of the services or may make the user experience less enjoyable.

2.6 Fulfilling our legal obligations

We process the data collected, to the extent necessary, including to comply with various legal requirements that apply to us, obligations that may include, as appropriate:

• issuing, registering and archiving invoices;

• calculation, reporting, payment of taxes and related fees and for various other tax issues;

• archiving the related documents;

• keeping the registers required by law;

• registration and archiving of agreements expressed by users;

• providing data to the Romanian authorities upon request or when required by law;

• providing data to users, upon request or in cases established by law, etc.

We base these processing on the need to comply with our legal obligations.

2.7 For carrying out legal proceedings

We can also process a series of data, depending on the specific situation, for:

• to analyze and resolve requests, notifications, complaints, disputes regarding our activity or the operation of the Platform

• to defend, preserve or exercise our rights, in all procedural phases: pre-litigation, litigation (mediation, courts, arbitration), enforcement

We base this processing mainly on our legitimate interest in protecting our business and commercial interests, ensuring that all the measures we take guarantee a balance between our interests and your fundamental rights and freedoms. Depending on the specific situation, we may rely on the processing of data for this purpose, to a limited extent and to the extent necessary, including the legitimate interest of others or the public interest.

Also, in some cases we base our processing on legal obligations, such as the obligation to make available to the judicial authorities the data they may request.

III. AUTOMATIC DATA PROCESSING. PROFILE CREATION

Please note that if you have entered the competition and the payment cannot be collected immediately after payment (for example, you have insufficient funds, the card is blocked, etc.), the use of the services provided by LPIN will be automatically restricted. (respectively participation in competitions or purchase of subscriptions or other services from the Platform) until the payment of those services. This processing is necessary in order to continue to provide our services.

You will be notified immediately at the e-mail address registered in the account, as well as, if you have given your consent, by a notification by phone.

If you wish to receive further information or object to the restriction, please contact us at any of the contact details at the end of this Policy (see Section XI - How you can exercise your rights). You can also add another payment card to your account at any time.

It is also possible to create profiles to monitor, prevent, detect and report fraud, in cases provided by law. Such incidents may lead to the deactivation of the user account or the blocking of the use of the Platform.

IV. THE RIGHT TO OPPOSE PROCESSING

Please note that for the data we process on the basis of LEGITIMATE INTEREST (as detailed above) you have the RIGHT to OPPOSE such processing for reasons related to your particular situation.

Please also keep in mind that you have the right to object when we process your personal data for the purpose of DIRECT MARKETING. Thus, you can oppose, at any time, the processing of your personal data for this purpose, including the creation of profiles, insofar as it is related to that direct marketing. If you object to the processing for direct marketing purposes, your personal data will no longer be processed for this purpose.

More information on the right to oppose can be found in Section X below, as well as in art. 21 of the GDPR.

V. THE RIGHT TO WITHDRAW CONSENT

We process the following types of data based on your prior consent:

• optional account data (phone, gender, photo), which either facilitates the use of the services offered or improves the experience the user

• phone or e-mail notifications regarding Marketing information such as offers, promotions, newsletters or similar (we process the phone number and / or e-mail)

Please note that you are not obliged to give us your consent to any of these processing. You can also use the services offered by the Platform if you do not agree to process any of this data. The choice is yours alone!

You may express or withdraw your consent at any time as follows:

• for optional account data (phone, gender, photo): you can choose to fill in the data when creating the account or you can fill in / modify this data by entering your user account, then in Account settings, then in My account.

• for phone notifications: you can set your preferences by logging in to your user account, then in Account settings, then in Privacy settings. There you can activate or deactivate the field I want to receive Information on the use of services.

• in the case of Marketing Information (commercial communications):

- you can choose to receive such information when you create your account

- You can accept or opt-out of such information at any time by logging into your user account, then in Account Settings, and then in Privacy Settings. You will be able to set your preferences through the dedicated field: I want to receive Marketing Information or

- you can subscribe to the Marketing Information, in the Subscribe to our newsletter section from the final part of our website www.lpin.ro

- you can also withdraw your consent by accessing the unsubscribe link displayed at the end of the emails we send you Marketing Information (this can be called unsubscribe or unsubscribe) and following the steps described in the link below. will open.

Please note, however, that due to technical processing times, sometimes a certain amount of time may be recorded between the time you have expressed your new option and the time it is fully implemented at the Platform level. Therefore, we cannot completely rule out that, within a short period of time after you have withdrawn your consent (which, in principle, should not exceed a few hours), we can continue processing and receive, for example, notifications by phone. or Marketing Information. We assure you that we will make every effort to ensure that this does not happen.

In the unlikely event that you continue to receive notifications by phone or Marketing Information after following any of the above steps, please contact us at contact@lpin.ro to ensure that your request is implemented.

Please note that the withdrawal of consent means that we will no longer be able to process such data later, using consent as a basis. However, depending on the circumstances, we may continue to process such data for limited purposes on other grounds, for example, in order to preserve, exercise or defend our rights in court, to fulfill certain legal obligations, or to other similar cases which are closely related to the initial processing.

In any case, please note that the withdrawal of consent does not affect the legality of the processing previously carried out on the basis of the consent expressed, nor the processing of data that is not carried out on the basis of the consent.

VI. DATA STORAGE PERIOD

6.1 The data related to your account in the Platform

We store your personal data, as a rule, for the entire period you have an LPIN account, as well as thereafter, as described below.

You can request to close your account at any time. To close the account, log in to your user account, then to Account settings, then to Privacy settings. At the end you will find the Close account field. Please note that after closing your account you will lose your account data.

Upon closing the account, some of the data associated with the account (such as photo, phone, country) will be deleted or, as appropriate, anonymized in the Platform.

Please note, however, that after closing your account, we may continue to process some of your user account data, either because the law requires us to keep certain data for certain periods or to make certain data available to the authorities, or for identification purposes. , fraud prevention and security, or to be able to preserve, exercise or defend our rights or interests, for example in case of disputes, investigations, fraud, as follows:

• the data from the invoices (name, surname, address, e-mail) but also the obligatory accounting records, as well as any other supporting documents that are the basis of the accounting records, or which are indicated by law - are kept for the period established by law ;

• the agreements and options expressed by the user, the e-mails and notifications sent to / received from the user, the correspondence with the user, as well as any other dwhich may be relevant in case of control / investigations by the competent authorities or in case of disputes / requests / complaints / etc. - it shall be kept for at least the general limitation period (or any other applicable limitation period) and, where appropriate, for the duration of the review, investigation or dispute (until all procedural steps have been completed);

• In general, we will continue to process the data to the extent required by law, for the period provided by law.

In order to limit to the strict necessary the data that we process after closing the account, we periodically check the need to continue processing after closing the account.

At the end of the processing period, your personal data will be securely deleted, destroyed or anonymized, within a reasonable period of time for the implementation of these measures.

6.2 Data collected or used by cookies or other similar means

This data is stored in accordance with the Cookies Policy, which you can consult for this purpose.

6.3 Other data

The data in the contact form, chat, messages, requests, requests or any other addresses you send us are kept until the issues that are subject to them are resolved, and then for the applicable general limitation period (as a rule 3 years), and if it is the case, for the entire duration necessary for the settlement of any disputes or related controls.

If the messages received have no content, the data are, as a rule, deleted within 3 months of receiving them, unless other purposes are necessary (for example, to defend our rights or to respond to other related requests).

VII. RECIPIENTS OF PERSONAL DATA

The personal data referred to in this Policy may, to a limited extent, be transmitted to / accessed by affiliated entities, service providers, employees of LPIN or other independent legal entities, but also to public authorities or institutions, such as:

• collaborators, service providers or other entities with which LPIN has concluded various service contracts or other types of contracts, which aim at the proper functioning and / or development of our activity (eg IT service providers, e-mail services and servers, marketing, analysis, web optimization and security, logistics, technical assistance, accounting and audit services, payment service banks / processors, market research service providers, insurers, couriers, etc.). Where appropriate, they may act as our operator or authorized person. In general, the access of these entities to personal data is restricted or limited to the minimum necessary for the provision of those services;

• lawyers, bailiffs and / or other external professional consultants. They generally have a legal obligation to maintain data confidentiality;

• public authorities, persons invested with public power, public institutions, relevant courts, etc., in Romania or abroad, in case of control, at their request or at our initiative, when we are obliged or to protect our rights and interests in accordance with applicable law. And in this case, we have in mind a limitation of personal data that are transmitted to the data strictly necessary for that purpose;

• potential buyers or investors if various types of transactions / operations of sale, merger, division, reorganization, etc. are analyzed, intended, negotiated, concluded or implemented. and LPIN. In general, the data provided are either statistical or anonymized, and where the transmission of personal data is required they will be limited to the minimum necessary for that purpose;

• other third parties, in the cases provided or permitted by law;

• in other cases, with your prior notice.

Please note that, depending on the specifics and the way of performing the services / activities provided and the related legal requirements, it is possible for any of these entities / persons to transmit the data thus obtained to public authorities, accountants, lawyers, courts. , other entities / persons, etc. (for example, everyone can have their own IT provider who may have limited access to data).

Also, keep in mind that our website uses cookies and similar technologies. To see where the data collected through them is transmitted, please access the Cookies Policy.

VIII. TRANSFER OF DATA TO RECIPIENTS FROM THIRD COUNTRIES OR INTERNATIONAL ORGANIZATIONS

For the safe and optimal operation of the Platform and the services provided through it, we use a series of services provided by well-known international companies that and are headquartered in the United States and Europe.

These services may have access to certain user information (for example, when checking the security of the site, or when using the chat service, etc.).

Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46 / EC of the European Parliament and of the Council on the adequacy of the adequacy of the European Union was published in the Official Journal of the European Union protection provided by the EU-US Privacy Shield. According to this decision, the United States guarantees an adequate level of protection of personal data transferred from the European Union to organizations in the United States under the EU-US Privacy Shield, provided that those entities process personal data in accordance with a a strong set of principles and guarantees for the protection of privacy and personal data that are equivalent to those in the European Union.

The text of the Commission Decision can be found at:

https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32016D1250&from=EN

A list of companies covered by the EU-US and Switzerland-US Privacy Shield is included on the US Department of Commerce website (https://www.privacyshield.gov/welcome).

All companies based in the United States of America from which we use services are included in this List, thus being subject to the EU-US Privacy Shield.

This is how we use:

• the server service is provided by Prime Telecom, based in Romania, Lascăr Catargiu Boulevard Nr. 34, Bucharest 010673, REGISTRATION NUMBER: J40 / 10171/2000, FISCAL CODE: 13506450.

The data is stored on the server in a data center in Romania.

• the web traffic analysis service is provided by Google Analytics, the Google service being owned by Google LLC. For users of the European Economic Area, Google services are provided by Google Ireland Limited, a company registered and operating under the laws of Ireland (registration number: 368047) and headquartered in Gordon House, Barrow Street, Dublin 4, Ireland.

According to Google, it has servers all over the world; the information collected may be processed by servers located in a country other than the one where you live. According to Google, no matter where the processing takes place, it offers the same level of protection as described in its privacy policy and respects the EU-US Privacy Shield.

At the date of this Policy, except as set forth above, we do not transfer or intend to transfer your personal data to entities or individuals outside the European Union or to international organizations. The collaborators, partners and, in general, the persons and entities that we contract directly and to which we directly transmit personal data are, as a rule, persons / entities from Romania or from the European Union. In any case, their access to data is generally extremely limited (to only what is possibly necessary for the provision of that service).

However, we cannot rule out that they transmit or process, in certain situations, your data in / from other countries, which may or may not be members of the European Union (for example, if they have servers located, in turn, at Microsoft). In the contractual clauses that we will conclude with them, we will ensure that these entities / persons assume the existence of adequate security measures and guarantees designed to ensure the confidentiality and proper protection of your personal data.

If LPIN transfers personal data to entities / persons outside the European Union, we will ensure that appropriate personal data protection measures are put in place, or we will ask for your consent to make such transfers, with your prior knowledge of the potential risks involved. In exceptional situations where it will be necessary to transfer data outside the European Union, and the above conditions are not met, we will ensure that the transfer will be made exclusively in cases where the law allows express derogations (eg Article 49 of the GDPR).

IX. DATA SECURITY

We have a strong and constant concern to ensure the security of your data.

First, your card data is processed through the secure payment processor platform, which has implemented specific security measures.

We have also taken appropriate technical and organizational measures to ensure the security of the data and to limit the risks that may arise from the destruction, loss, alteration, unauthorized disclosure or unauthorized access to personal data transmitted, stored or processed in a other way.

LPIN uses advanced security methods and technologies, has implemented internal policies and working procedures to protect the processing of personal data and constantly analyzes the observance and protection of the security of the data and systems used.

Please note that due to the way personal data is transmitted and processed electronically, there may be a risk of interception, loss, copying, blocking of data and information. We cannot guarantee the absolute security of the data during transmission or storage in our systems. We have taken steps to identify any attempts to gain unauthorized access to our database. We cannot be held responsible for vulnerabilities in systems that are not under our control, nor for errors in user negligence regarding the security and privacy of email, account and password used, or devices and networks used to transmit data.

In the event of a security breach, we consider reporting these incidents to the appropriate authorities, and will inform you directly as appropriate (via email, in-app notifications, or other available means).

X. YOUR RIGHTS IN RELATION TO THE OPERATOR, REGARDING DATA PROCESSING

You have the following main rights, which you can exercise, under the conditions established by law (these rights are established in art. 12-22 of the GPDR):

• the right to access data (art. 15 of the GDPR): you have the right to obtain from us a confirmation that personal data concerning you are processed or not and, if so, access to those data and the following information :

- purposes of processing;

- the categories of personal data concerned;

- recipients or categories of recipients to whom personal data have been or are to be disclosed, in particular recipients from third countries or international organizations;

- where possible, the period for which personal data are expected to be stored or, if this is not possible, the criteria used to establish this period;

- the existence of the right to request the operator to rectify or delete personal data or to restrict the processing of personal data concerning the data subject or the right to oppose the processing;

- the right to lodge a complaint with a supervisory authority;

- if personal data are not collected from the data subject, any available information on their source;

- the existence of an automated decision-making process including profiling (referred to in Article 22 (1) and (4) of the GDPR), as well as, at least in those cases, relevant information on the logic used and on the importance and expected consequences of such processing for the data subject. In this case, if the processing is performed by automatic means you have the right not to be subject to an individual decision.

- if personal data are transferred to a third country or an international organization, you have the right to be informed of the appropriate safeguards regarding the transfer (pursuant to Article 46 of the GDPR).

Without prejudice to the rights and freedoms of others, you have the right to obtain a copy of the personal data subject to processing.

Before you submit this request to us, please note that the Report will contain personal data about you that needs to be protected. Carefully check the security of the networks, devices, and services you use to store or transmit this data. For added security, after completing the intended actions with your data, you may delete or secure, in any other way, the email you received and the downloaded files containing your personal data from your device.

Please note that in addition to the information generated in this Report, we may also process other data about you (for example, if we have corresponded with you separately). To learn more about the data we process about you, see How you can exercise your rights.

• the right to rectification of data (art. 16 of the GDPR): you have the right to obtain from us, without undue delay, the rectification of inaccurate data concerning you; Depending on the purposes for which the data are processed, you have the right to obtain the completion of personal data that are incomplete, including by providing an additional statement.

We must communicate to each recipient to whom we have disclosed the personal data any rectification of the personal data, unless this proves impossible or involves disproportionate efforts. If you request this, you will m inform about the respective recipients.

• the right to delete data ("the right to be forgotten") (art. 17 of the GDPR): you have the right to obtain from us the deletion of personal data concerning you, and we have the obligation to delete data without undue delay , if one of the following reasons applies:

- personal data are no longer necessary for the purposes for which they were collected or processed;

- withdraw your consent on the basis of which the processing takes place and there is no other legal basis for the processing;

- you object to the processing pursuant to art. 21 paragraph (1) of the GDPR - ie for reasons related to the particular situation you are in, when, for example, the processing is done on the basis of legitimate interest (details can be found below) and there are no legitimate reasons prevailing in regarding processing;

- you object to the processing pursuant to art. 21 paragraph (2) of the GDPR - ie when the processing of personal data is aimed at direct marketing (details can be found below);

- personal data have been processed illegally;

- personal data must be deleted in order to comply with a legal obligation incumbent on us under Union or national law to which the controller is subject;

- personal data have been collected in connection with the provision of information society services directly to a child (referred to in Article 8 (1) of the GDPR), which in our case should not happen.

If we have made personal data public and we are obliged to delete it, we must, taking into account the available technology and the cost of implementation, take reasonable steps, including technical measures, to inform the operators processing the personal data that you have requested. the deletion by these operators of any links to such data or of any copies or reproductions of such personal data.

Please note that in certain cases expressly permitted by law (in Article 17 paragraph (3) of the GDPR), we may not delete the data (for example, if we have to keep them in order to comply with a legal obligation, such as the data in the invoices that we have to keep for the period established by law).

We must also communicate to each recipient to whom we have disclosed personal data any deletion of the data, unless this proves impossible or involves disproportionate effort. If you request this, we will inform you about the respective recipients.

• the right to restrict data processing (art. 18 of the GDPR): you have the right to obtain from us the restriction of your data processing if one of the following cases applies:

- if you challenge the accuracy of the data, for a period that allows us to verify the accuracy of the data;

- the processing is illegal and you object to the deletion of personal data, instead requesting a restriction on their use;

- we no longer need personal data for the purpose of processing, but you request them for us to establish, exercise or defend a right in court; or

- you objected to the processing in accordance with art. 21 para. (1) of the GDPR (ie for reasons related to the particular situation you are in, when, for example, processing is done on the basis of legitimate interest) for the period of time in which it is verified whether our legitimate rights prevail over your rights.

We must communicate to each recipient to whom we have disclosed personal data any restriction on the processing carried out, unless this proves impossible or involves disproportionate efforts. If you request this, we will inform you about the respective recipients.

• the right to data portability (art. 20 of the GDPR): you have the right to receive personal data concerning you and which you have provided to us in a structured format, commonly used and which can be read automatically and you have the right to transmit this data to another operator, without hindrance on our part, if:

- processing is based on consent or a contract

- the processing is performed by automatic means.

You also have the right to have personal data transmitted directly from one operator to another where this is technically feasible.

You can exercise your right to data portability by logging in to your user account, then to Account settings, and then to Privacy settings. In the final part enter the field: Request personal data and follow the instructions there. You will receive, in a very short time, by e-mail, a Report with the personal data processed within the Platform. The report will not include data that has been deleted or modified.

Before send us this request, please note that the Report will contain personal data concerning you and which must be protected. Carefully check the security of the networks, devices, and services you use to store or transmit this data. For added security, after completing the intended actions with your data, you may delete or secure, in any other way, the received email and downloaded files containing your personal data from your device.

• the right to oppose the processing (art. 21 of the GDPR): you have the right to oppose, at any time, for reasons related to the particular situation you are in, the processing of personal data concerning you under art. 6 para. (1) lit. (e) of the GDPR (ie when the processing is carried out to perform a task which serves a public interest or which results from the exercise of the public authority with which the operator is vested) or letter (f) (ie when the processing is carried out for the legitimate interests of the controller or a third party), including the creation of profiles on the basis of those provisions.

In this case, we no longer process personal data, unless we can demonstrate that we have legitimate and compelling reasons justifying the processing and prevailing over your interests, rights and freedoms or that the purpose is to establish, exercise or defend a right. in court.

You also have the right to object at any time to the processing of personal data concerning you carried out for the purpose of direct marketing, including the creation of profiles, insofar as it relates to that direct marketing. In this case, personal data are no longer processed for this purpose.

Please note that in the emails we send you Marketing Information, you will find a unsubscribe link at the end (this can be called unsubscribe or unsubscribe). If you no longer wish to receive such emails, please enter that link and follow the steps outlined in it.

XI. HOW YOU CAN EXERCISE YOUR RIGHTS.

To exercise your rights, see Section X above, where we've explained exactly how you can exercise certain rights directly from your account.

You can also send us any request, question or question regarding any of these rights, at the following contact details:

• Address: 32E Hipodromului Street, Corbeanca Commune, Ilfov County, Romania.

• E-mail: contact@lpin.ro

Please note that the submission of these requests involves further processing of your data.

In order to respond to requests, we may request additional information necessary to confirm your identity.

We are convinced that you will not exercise these rights unreasonably, excessively or abusively.

XII. THE RIGHT TO SUBMIT A COMPLAINT TO THE SUPERVISORY AUTHORITY

If you consider that we do not comply with data protection legislation, you have the right to lodge a complaint with the data supervisory authority.

In Romania this is:

National Authority for the Supervision of Personal Data Processing (ANSPDCP).

As of this date, ANSPDCP has the following contact details:

Headquarters: Bd. Gheorghe Magheru no. 28-30, Bucharest, Sector 1, postal code 010336, Romania

E-mail: anspdcp@dataprotection.ro

Fax: +40.318.059.602

Website: www.dataprotection.ro