General Data Protection Regulation – FIRE Group LTD / FIRE Token Platform

Overview

This privacy policy concerns FIRE GROUP LTD., 26th Floor The H Hotel Office Tower, One Sheikh Zayed Road, P.O. Box 62201 Dubai, United Arab Emirates and its affiliates. This Privacy Policy explains how we may use information that we obtain about you through your use of our websites (our "Site") and other sources and outlines FIRE Group´s duties of Transparency under the General Data Protection Regulation (GDPR).

Marketing Communications Preferences

You may request us to stop sending you marketing messages at any time by following the opt-out links on any marketing message sent to you, or by contacting us at any time at ***support@fire-token.com***.

Data protection officer (Art. 32 DSGVO)

If you have any questions or comments concerning this privacy policy or our handling of personal data, please address your request to:

FIRE GROUP LTD.
26th Floor The H Hotel Office Tower
One Sheikh Zayed Road
P.O. Box 62201 Dubai
United Arab Emirates
Email: gdpr@fire-token.com

What Personal Data We Collect

When you use our Site or when we interact with you, the Personal Data we collect, may include:

- Contact Data, such as your name, job title, business address, telephone number, mobile phone number, email address, and social media profiles.
- Profile and Usage Data, including passwords to our Site or password protected platforms or services, your preferences in receiving marketing information from us, your communication preferences and information about how you use our Site including the services you viewed. To learn more about our use of cookies or similar technology please check our Cookies policy
- Technical Data, including Internet protocol (IP) address, your login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform, and other technology on the devices you use to access our Site or use our services.
- Know Your Customer (KYC) data required to identify prospective investors in order to comply KYC and anti-money Laundering and Terrorist Financing (AML) laws and regulations. Information required for this purpose will include formal identification information, including passport number, driver's license details, national identity card details, video identification data, photograph identification cards, and/or resident permit (visa) information. To learn more about the data collected for KYC and AML purposes please check our KYC/AML data privacy policy.
- Financial Information: Bank account information, payment card primary account number (PAN), transaction history, trading data, crypto wallet information, and/or tax identification.
- Transaction Information: Information about the transactions you make on our Services, such as the name of the recipient, your name, the amount, and/or timestamp.

We may also collect Personal Data from third party partners and public sources as required or permitted by applicable law, such as public databases, credit bureaus, ID verification partners, resellers and channel partners, joint marketing partners, and social media platforms.

We use public databases and ID verification partners to verify your identity. ID verification partners use a combination of government records and publicly available information about you to verify your identity. Such information includes your name, address, job position, public employment profile, credit history, status on any sanctions lists maintained by public authorities, and other relevant data. We obtain such

information to comply with our legal obligations, such as anti-money laundering laws.

In some cases, we may process additional data about you to ensure our services are not used fraudulently or for other illicit activities. In such instances, processing is necessary for us to continue to perform our contract with you and others.

How We Use Your Personal Data

In general, we use personal information to create, develop, operate, deliver, and improve our Services, content and advertising, and for loss prevention and anti-fraud purposes. We may use this information in the following ways:

- **To Maintain Legal and Regulatory Compliance**

Some of our services are subject to laws and regulations requiring us to collect and use your personal identification information, formal identification information, financial information, transaction information, employment information, online identifiers, and/or usage data in certain ways.

We must identify and verify prospective investors in order to comply with anti-money laundering and terrorist financing laws across jurisdictions. In addition, we use third parties to verify your identity by comparing the personal information you provided against third-party databases and public records.

We may require you to provide additional information which we may use in collaboration with service providers acting on our behalf to verify your identity or address, and/or to manage risk as required under applicable law. If you do not want to have your personal information processed for such purposes, then we shall terminate your account as we cannot perform the services in accordance with legal and regulatory requirements.

- **To Enforce Our Terms in Our User Agreement and Other Agreements**

We handle sensitive information, such as your identification and financial data, so it is very important for us and our customers that we are actively monitoring, investigating, preventing and mitigating any potentially prohibited or illegal activities, enforcing our agreements with third parties, and/or violations of our posted user agreement or agreement for other services. We collect information about your account usage and closely monitor your interactions with our services. The consequences of not processing your personal information for such purposes is the termination of your account as we cannot perform our services in accordance with our terms.

- **To Provide FIRE TOKEN Services**

We process your personal information in order to provide the services to you, in particular in order got grant access to the FIRE TOKEN eco system. We cannot provide you with services without such information.

- **To Provide Service Communications**

We send administrative or account-related information to you to keep you updated about our services, inform you of relevant security issues or updates, or provide other transaction-related information. Without such communications, you may not be aware of important developments relating to your account that may affect how you can use our services.

- **To Provide Customer Service**

We process your personal information when you contact us to resolve any question, dispute, collected fees, or to troubleshoot problems. We may process your information in response to another customer's request, as relevant. Without processing your personal information for such purposes, we cannot respond to your requests and ensure your uninterrupted use of the services.

- **To Ensure Quality Control**

We process your personal information for quality control and staff training to make sure we continue to provide you with accurate information. If we do not process personal information for quality control purposes, you may experience issues on the Services such as inaccurate transaction records or other interruptions. Our basis for such processing is based on the necessity of performing our contractual obligations with you.

- **To Ensure Network and Information Security**

We process your personal information in order to enhance security, monitor and verify identity or service access, combat spam or other malware or security risks and to comply with applicable security

laws and regulations. The threat landscape on the internet is constantly evolving, which makes it more important than ever that we have accurate and up-to-date information about your use of our services. Without processing your personal information, we may not be able to ensure the security of our services.

- **For Research and Development Purposes**

We process your personal information to better understand the way you use and interact with our services. In addition, we use such information to customize, measure, and improve the Services and the content and layout of our website and applications, and to develop new services. Without such processing, we cannot ensure your continued enjoyment of our services. Our basis for such processing is based on legitimate interest.

- **To Enhance Your Website Experience**

We process your personal information to provide a personalized experience and implement the preferences you request. For example, you may choose to provide us with access to certain personal information stored by third parties. Without such processing, we may not be able to ensure your continued enjoyment of part or all of our services.

- **To Facilitate Corporate Acquisitions, Mergers, or Transactions**

We may process any information regarding your account and use of our services as is necessary in the context of corporate acquisitions, mergers, or other corporate transactions. You have the option of closing your account if you do not wish to have your personal information processed for such purposes.

- **To Engage in Marketing Activities**

Based on your communication preferences, we may send you marketing communications to inform you about our events or our partner events; to deliver targeted marketing; and to provide you with promotional offers based on your communication preferences. We use information about your usage of our services and your contact information to provide marketing communications. You can opt-out of our marketing communications at any time.

If you are a current customer residing in the EEA, we will only contact you by electronic means (email or SMS) with information about our services that are similar to those which were the subject of a previous sale or negotiations of a sale to you.

If you are a new customer and located in the EEA, we will contact you if you are located in the EU by electronic means for marketing purposes only if you have consented to such communication. If you do not want us to use your personal information in this way, or to pass your personal information on to third parties for marketing purposes, please follow the opt-out links included in marketing communications or contact us at *gdpr@fire-token.com*. You may raise such objection with regard to initial or further processing for purposes of direct marketing, at any time and free of charge. Direct marketing includes any communications to you that are only based on advertising or promoting products and services.

We will not use your personal information for purposes other than those purposes we have disclosed to you, without your permission. From time to time we may request your permission to allow us to share your personal information with third parties. You may opt out of having your personal information shared with third parties or allowing us to use your personal information for any purpose that is incompatible with the purposes for which we originally collected it or subsequently obtained your authorization. If you choose to so limit the use of your personal information, certain features or our Services may not be available to you.

On which legal basis do we use your personal data?

We process your personal data on the following legal basis according to Article 6. GDPR:

- Performance of our contract with you
- Compliance with legal obligations
- Legitimate interests of us or a third party
- With your express consent
- Other legal bases according to Article 6. GDPR

How long do we retain your personal data?

FIRE Group will retain your Personal Data only for as long as is necessary for the purposes set out in this Privacy Policy.

FIRE Group will retain and use your Personal Data to the extent necessary to comply with our legal obligations (for example, if we are required to retain your Data to comply with applicable laws), resolve disputes, and enforce our legal agreements and policies.

Therefore, and in accordance with our record keeping obligations, we will retain Account and other Personal Data for at least five years (and some up to ten years, as required by applicable law) after an Account is closed.

FIRE Group will also retain Data Collected Automatically either generated by the use of the website or from the website infrastructure itself (for example, the duration of a page visit) for internal analysis purposes.

This Data is generally retained for a shorter period of time, except when this Data is used to strengthen the security or to improve the functionality of our Service, or we are legally obligated to retain this Data for longer time periods.

Hence, this kind of Data collected via technical means such as cookies, webpage counters and other analytics tools is normally kept for a period of up to one year from expiry of the cookie.

What are your rights regarding your personal data?

With regard to your personal data being processed you have the following rights:

- Right of Information: You have the right to request information about your personal data that is processed by us.
- Right of Rectification: You have the right to obtain from us without undue delay the rectification of inaccurate personal data concerning you.
- Right of Erasure: You can demand that we delete your personal data if your data is no longer necessary for the purposes for which it was collected or processed, if you have revoked your consent or if the data is processed unlawfully. There is no right of erasure, if the processing of the data is necessary due to a legal obligation or the assertion, exercise or defense of legal claims.
- Right to restriction of processing: You have the right to restrict the processing of your personal data with regard to the transmission of such data to third parties. Such restriction may conflict with legal regulations. In such cases, we will only transmit your personal data to third parties to the extent necessary to comply with the statutory requirements.
- Right to data portability: You have the right to receive the personal data concerning you, which you have provided to us, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from us, if the processing is based on your consent and the processing is carried out by automated means.
- Right of objection: You have the right to withdraw your consent to the processing of personal data concerning you for one or more specific purposes at any time if the processing is based on your express consent.

If you object to the processing of your Personal Data, or if you have provided your consent to processing and you later choose to withdraw it, we will respect that choice in accordance with our legal obligations.

Your objection (or withdrawal of any previously given consent) could mean that we are unable to perform the actions necessary to achieve the purposes set out above (see "How We Use Your Personal Data"), or that you may not be able to make use of the services and products offered by FIRE Group. Please note that even after you have chosen to withdraw your consent we may be able to continue to process your Personal Data to the extent required or otherwise permitted by law, in particular in connection with exercising and defending our legal rights or meeting our legal and regulatory obligations. If you have provided your consent and wish to withdraw your consent, please follow the opt-out links on any marketing message sent to you or contact us at *gdpr@fire-token.com*.

Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose(s) to which you originally consented, unless there are compelling legitimate grounds for further processing which override your interests, rights, and freedoms or for the establishment, exercise, or defense of legal claims. Withdrawal of consent to receive marketing communications will not affect the processing of Personal Data necessary for us to provide products

or services to you necessitated by any contractual relationship you or your firm has with FIRE Group.

We must ensure that your Personal Data is accurate and up to date, where relevant. Therefore, please advise us of any changes to your information by emailing us at ***gdpr@fire-token.com*** .

If you would like to make a complaint regarding this Privacy Policy or our practices in relation to your Personal Data, please contact us at ***gdpr@fire-token.com***. We will reply to your complaint as soon as we can.

If you feel that your complaint has not been adequately resolved, please note that the GDPR gives you without prejudice to other administrative or judicial remedies, the right to complain to the responsible data protection supervisory authority:

In Dubai the UAE Central Bank is responsible for its Consumer Protection Regulation and Standards, and the SVF Regulation.

Central Bank of the UAE
next to King Abdullah Bin Abdulaziz Al Saud Street - Al Bateen - W34
Abu Dhabi
Vereinigte Arabische Emirate
Phone: +971 2 691 5555
https://crm.centralbank.ae/en

Links to third party websites

On our website you will find Links to a number of third-party websites (e.g. Facebook, Twitter, Instagram, Youtube etc.). No data will be transferred by us via these Links to the respective owner of the website. Please review the privacy statements of the linked websites carefully before disclosing any personal information.

Data Security

We store all your Personal Data on servers operated by Microsoft Office 365, Switzerland, (Client data, KYC data, Webpage and Fire Group entity server) and by KORE, Switzerland (Smartcontract, Blockchain, Backend - FIRE Token platform). Marketing data is furthermore stored at servers in Germany.

All Personal datas of citizen of European Countries (incl. EWG and European Union) and Switzerland we store sole to Servers located in European Countries. Datas of these Persons doesn´t leave European Countries.

We take all reasonable effort on technical and organizational security measures to protect your Data from being manipulated, lost or accessed by unauthorized third-parties.

Our website is scanned on a regular basis for security holes and known vulnerabilities in order to make your visit to our Site as safe as possible.

Your Personal Data is contained behind secured networks and is only accessible by a limited number of individuals who have special access rights to such systems and are required to keep the information confidential.

Although no method of transmission over the Internet, or method of electronic storage is one hundred percent secure, we strive to continually update and improve our security measures with the most recent technological developments.

We would like to draw your attention on the fact that we normally never ask for financial or payment information, such as your credit card number, passcode, account number or pin number, in an e-mail, text or any other communication that we send to you. Please always check that any website on which you are asked for financial or payment information in relation to our reservations or services is operated by Mt Pelerin. The risk of impersonating hackers exists and should be taken into account when using our website and/or Services.

If you do receive a suspicious request, do not provide your information and report it by contacting one of our member service representatives as set in this Privacy Policy.

Since we cannot 100% guarantee that loss, misuse, unauthorized acquisition, or alteration of your data will not occur, please accept that you play a vital role in protecting your own Personal Data. When registering with us, it is important to choose an appropriate password of sufficient length and complexity, to not reveal this password to any third-parties, and to immediately notify us if you become aware of any

unauthorized access to or use of your account.

Furthermore, we cannot ensure or warrant the security or confidentiality of information you transmit to us or receive from us by Internet or wireless connection, including email, phone, or SMS, since we have no way of protecting that information once it leaves and until it reaches us. If you have reason to believe that your data is no longer secure, please contact us at the email address, mailing address or telephone number listed at the end of this Privacy Policy.

Personal data transfer to third parties

We may disclose your Personal Data to third parties and legal and regulatory authorities, and transfer your Personal Data outside the EEA, as described below.

There are certain circumstances where we may transfer your personal data to employees, contractors and to other parties like KYC Service providers and/or Payment Service Providers.

We may share information about you with other members of our group of companies, so we can provide the best service across our group. They are bound to keep your information in accordance with this Privacy Policy;

We may also share your information with certain contractors or service providers. They may process your personal data for us in particular for customer identification as part of the KYC process, for the screening of customers or transactions in order to implement AML policies. Customer and financial data will furthermore be processed by paying agents. Other recipients/service providers include advertising agencies, IT specialists, database providers, backup and disaster recovery specialists, email providers or outsourced call centers. Our suppliers and service providers will be required to meet our standards on processing information and security. The information we provide them, including your information, will only be provided in connection with the performance of their function;

We may also share your information with certain other third parties. We will do this either when we receive your consent or because we need them to see your information to provide products or services to you. These include credit reference agencies, anti-fraud databases, screening agencies and other partners we do business with.

Your personal data may be transferred to other third-party organizations in certain scenarios:

- If we're discussing selling or transferring part or all of our business – the information may be transferred to prospective purchasers under suitable terms as to confidentiality;
- If we are reorganized or sold, information may be transferred to a buyer who can continue to provide services to you;
- If we're required to by law, or under any regulatory code or practice we follow, or if we are asked by any public or regulatory authority – for example the Police;
- If we are defending a legal claim your information may be transferred as required in connection with defending such claim.
- Your personal data may be shared if it is made anonymous and aggregated, as in such circumstances the information will cease to be personal data.

Your information will not be sold, exchanged, or shared with any third parties without your consent, except to provide our services or as required by law.

If a service provider is located in a country that does not apply the standard of data protection of Swiss law and EU General Data Protection Regulation, FIRE Group will use a contract to ensure that your Personal Data has the same level of protection as if protected in accordance with Swiss Federal Act on Data Protection and its Ordinance and EU General Data Protection Regulation (see point XII.).

Do we transmit personal data to third countries?

We store and process your Personal Data in data centers around the world, wherever our service providers are located.

As such, we may transfer your Personal Data outside of Switzerland or the European Union. In these cases, the transfer is usually based on an adequacy decision of the European Commission (Art.45 GDPR) or appropriate safeguards (Art. 46 GDPR). The specific countries where adecquacy decisions have been resolved can be found here: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-

outside-eu/adequacy-protection-personal-data-non-eu-countries_en. We will also transfer the data to third countries if you have consented to the transfer of the data, or if we are entitled to the transmission for another reason according to Article 49 GDPR.

Do we use Cookies?

This website uses cookies. By using the website and agreeing to this policy, you consent to our use of cookies in accordance with the terms of this policy.

ABOUT COOKIES

Cookies are files, often including unique identifiers, that are sent by web servers to web browsers, and which may then be sent back to the server each time the browser requests a page from the server.

Cookies can be used by web servers to identity and track users as they navigate different pages on a website, and to identify users returning to a website.

Cookies may be either "persistent" cookies or "session" cookies. A persistent cookie consists of a text file sent by a web server to a web browser, which will be stored by the browser and will remain valid until its set expiry date (unless deleted by the user before the expiry date). A session cookie, on the other hand, will expire at the end of the user session, when the web browser is closed.

COOKIES ON THE WEBSITE

We use both session cookies and persistent cookies on the website.

HOW WE USE COOKIES

Cookies do not contain any information that personally identifies you, but personal information that we store about you may be linked, by us, to the information stored in and obtained from cookies. The cookies used on the website include those which are strictly necessary cookies for access and navigation, cookies that track usage (performance cookies), remember your choices (functionality cookies), and cookies that provide you with targeted content or advertising

We may use the information we obtain from your use of our cookies for the following purposes:

to recognise your computer when you visit the website;

to track you as you navigate the website, and to enable the use of any e-commerce facilities;

to improve the website's usability

to analyse the use of the website

in the administration of the website

to personalise the website for you, including targeting advertisements which may be of particular interest to you.

The legal basis for the data processed by cookies is Article 6 para. 1 f) GDPR.

THIRD PARTY COOKIES

When you use the website, you may also be sent third party cookies. We only use third-party cookies with your express consent.

Our advertisers and service providers may send you cookies. They may use the information they obtain from your use of their cookies:

to track your browser across multiple websites

to build a profile of your web surfing

to target advertisements which may be of particular interest to you.

In addition to the information we provide in this Cookie Policy, you can find out more information about your online choices at ***http://www.youronlinechoices.eu***

BLOCKING COOKIES

Most browsers allow you to refuse to accept cookies. For example:

in Internet Explorer you can refuse all cookies by clicking "Tools", "Internet Options", "Privacy", and selecting "Block all cookies" using the sliding selector;

in Firefox you can block all cookies by clicking "Tools", "Options", and un-checking "Accept cookies from sites" in the "Privacy" box.

in Google Chrome you can adjust your cookie permissions by clicking "Options", "Under the hood",

Content Settings in the "Privacy" section. Click on the Cookies tab in the Content Settings.

in Safari you can block cookies by clicking "Preferences", selecting the "Privacy" tab and "Block cookies".

Blocking all cookies will, however, have a negative impact upon the usability of many websites. If you block cookies, you may not be able to use certain features on the website (log on, access content, use search functions).

DELETING COOKIES

Cookies are stored until they are deleted by you.

You can delete cookies in the following ways:

in Internet Explorer, you must manually delete cookie files;

in Firefox, you can delete cookies by, first ensuring that cookies are to be deleted when you "clear private data" (this setting can be changed by clicking "Tools", "Options" and "Settings" in the "Private Data" box) and then clicking "Clear private data" in the "Tools" menu.

in Google Chrome you can adjust your cookie permissions by clicking "Options", "Under the hood", Content Settings in the "Privacy" section. Click on the Cookies tab in the Content Settings.

in Safari you can delete cookies by clicking "Preferences", selecting the "Privacy" tab and "Remove All Website Data".

Website analytics, tracking

Google Analytics: This website uses Google Analytics, a web analytics service provided by Google Inc. ("Google"). Google Analytics uses so-called "cookies", text files that are stored on your computer and that allow an analysis of the use of the website by you. The information generated by the cookies about your use of the website is transmitted to a Google server in the USA and stored there. The IP address provided by Google Analytics as part of Google Analytics will not be consolidated with other Google data. On this website, we have also added the code "anonymizeIP" to Google Analytics. This guarantees the masking of your IP address so that all data is collected anonymously.

On our behalf, Google will use this information to evaluate the use of the website, to compile reports on website activity and to provide other services related to website usage and internet usage to the website operator. You can prevent the storage of cookies by a corresponding setting of your browser software; however, please note that in this case you may not be able to use all features of this website to the fullest extent.

You may also prevent the collection / transmission by Google of the data generated by the cookies and related to your use of the website (including your IP address) as well as the processing of this data by Google by downloading and installing the browser plug-in available at the following link: ***http://tools.google.com/dlpage/gaoptout?hl=en***.

The data linked with cookies is automatically deleted by Google after 26 months. The deletion of data whose retention period has been reached is done automatically once a month.

Facebook: We use the "Facebook Pixel" developed by Facebook, Inc. (1601 S. California Ave, Palo Alto, CA 94304, USA). This feature makes it possible to track the behavior of users who have clicked on a Facebook ad and been directed to the website of the provider in question. The effectiveness of Facebook ads can then be assessed for statistical and market research purposes, which in turn can help optimize future advertising measures. The data we obtain through this process is anonymous, meaning it gives us no means of tracing the identity of any user. This information is stored and processed by Facebook on servers in Princeville, Oregon (USA), in order to facilitate a connection to each user's profile. Facebook can then use the data for its own advertising purposes in line with its data usage guidelines (***https://www.facebook.com/about/privacy/***). As a result, Facebook and its partners can insert ads both on and outside of Facebook. A cookie may also be stored on your computer for these purposes. In your browser's settings, you can allow or deny cookies as a general rule. Please note, however, that doing so may prevent you from enjoying the full functionality of this website.

LinkedIn: Our online presence uses the "LinkedIn Insight Tag" of the network LinkedIn. Provider is the LinkedIn Corporation, 2029 Stierlin Court, Mountain View, CA 94043, USA. We use the LinkedIn Insight Tag to track conversions, retarget website visitors, and unlock additional insights about members interacting with our LinkedIn adverts. The LinkedIn Insight Tag enables the collection of metadata such as IP address information, timestamp, and events such as page views. All data is encrypted. The LinkedIn

browser cookie is stored in a visitor's browser until they delete the cookie or the cookie expires. With the help of the LinkedIn Insight Tag we are able to analyse the success of our campaigns within the LinkedIn platform or determine target groups for them based on the interaction of the users with our website. If you are registered with LinkedIn, it is possible for LinkedIn to associate your interaction with our online services with your user account.

LinkedIn is certified under the Privacy Shield Agreement and therefore guarantees compliance with European data protection legislation. You can permanently opt out on this link: ***https://www.linkedin.com/psettings/guest-controls/retargeting-opt-out***. For more information on the Linkedin Privacy Policy, go to: ***https://www.linkedin.com/legal/privacy-policy***. LinkedIn advertising cookie is used on the basis of Art. 6 (1) (f) GDPR. We have a legitimate interest in analyzing user behavior to optimize our website and advertising.

Google Ads Tracking: We use the Google AdWords service from Google. Our website uses the remarketing function of Google AdWords. This function serves to present interest-related advertisements to visitors of the website within the Google advertising network. According to its own statements, Google does not collect any personal data during this process. Further information on Google Remarketing and the Google privacy policy can be found at: ***http://www.google.com/privacy/ads/***.

Google Tag Manager: Our website uses Google Analytics and Google Tag Manager, web analytics services provided by Google Inc, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA (hereinafter: „Google"). The information generated by Google Analytics and Google Tag Manager by the cookie about your use of our website is sent to a Google server in the USA and stored there. On behalf of the operator of this website, Google will use this information for the purpose of evaluating your use of the website, compiling reports on website activity and providing other services relating to website activity and internet usage for the website operator. The IP address transmitted by your browser in the context of Google Analytics and Google Tag Manager is not merged with other data from Google. You can find more information about this at: ***https://policies.google.com/privacy?hl=en***

fusedeck: Our website uses "fusedeck", a tracking solution provided by Capture Media AG (hereinafter referred to as "Capture Media"). Capture Media is a Swiss company having its registered office in Zurich which, on behalf of its customers, measures website usage in the context of engagements and events. Tracking is anonymous so that it is impossible to attribute any information gained to any identified or identifiable persons.

For more information on data protection and the rights which data subjects have in connection with "fusedeck", including their right to "opt out" (right to object), please refer to the Privacy Policy and the Information on the Right to Object.

https://privacy.fusedeck.net/en/MsGStHOtsv

KYC/AML data privacy policy

Fire Group is required to identify prospective investors before any investment is made (Know your Customer, KYC). Prospective investors are also subject to reviews and checks in in order to prevent money laundering and terrorist financing (AML). This statement describes how data is collected and processed for this purpose.

Fire Group engages service providers to perform KYC and AML reviews. The service providers are data processor which means that they process Personal Data on behalf of the Fire Group. Service provides may use sub-processors. Prior to working with any service provider Fire Group ensures that they comply with the GDPR or any other relevant data protection legislation that may be applicable.

Prospective investors must provide personal data to us in order to be identified through the submission of information, forms or documents (in whatever format) through an upload to our website, use of our mobile application or otherwise. Personal Data we process enables us to identify the Customers either directly or indirectly by reference to an identifier. Examples of identifiers we process are name, identification number, passport or ID photograph, location data, an online identifier or one or more factors relating specifically to the economic or social identity of the natural person ("Personal Data"). Depending on certain criteria investor identification will also require an online video verification which will be stored by the service provider during the Securities Token Offering (STO) and afterwards only by Fire Group.

The result of the verification process, as well as all details and documents provided by investors to the service provider via the Site or a service provider website, mobile application or otherwise are available solely to service provider with whom the investor is engaging. The Personal Data is provided as part of the FIRE Token collation and evaluation of due diligence documentation on potential new and existing

investors to comply with applicable AML legislation.

For the purposes of GDPR, it should be noted that Personal Data may be transferred or accessed outside the European Economic Area ("EEA") at the request of FIRE Group. For prospective investors who are not resident within the EEA, you should note that there is a possibility your Personal Data will be transferred outside your country of residence. You should consult with the relevant contact at FIRE Group for further details in relation to jurisdictions used for the transfer of your Personal Data.

Do we add changes to this privacy policy?

FIRE Group may update the Privacy Policy from time to time. You shall be notified by or by any means of a notice on our services prior to the change becoming effective.

The changes of the Privacy Policy shall also be posted on this page.

You are advised to review this Privacy Policy periodically for any changes. Changes to this Privacy Policy are effective when they are posted on this page.