

# Lympid Privacy Policy

For end investors using Lympid-powered white-label investment interfaces

Controller: LYMPID LABS, LDA

Primary contact: [client.journey@lympid.io](mailto:client.journey@lympid.io)

Website: [lympid.io](https://lympid.io)

Main role: White-label fintech platform operator and tied agent of BMCP for relevant flows

Other parties: BMCP, Tradevest, Sumsb and other licensed partners may also process data

Audience: End investors and prospective investors

This document is drafted for investor-facing acceptance and disclosure. It should be reviewed together with each relevant product's subscription package, KID or equivalent disclosure, and any BMCP or licensed-partner terms.

## 1. Scope of this Privacy Policy

This Privacy Policy explains how LYMPID LABS, LDA ("Lympid", "we", "us" or "our") collects, uses, stores, shares and otherwise processes personal data when you access or use any investor portal, onboarding flow, website, application, communication channel or service operated by Lympid or made available through Lympid's white-label infrastructure under a client's brand.

This policy is intended for end investors and prospective investors. It applies whether you interact directly with a Lympid-branded interface or with a white-label environment presented under the brand of one of Lympid's clients.

Lympid acts as a tied agent of Black Manta Capital Partners GmbH ("BMCP") and works with licensed or specialised partners, including for onboarding, KYC/AML, payment, custody, execution, registry, digital signature and compliance services. Depending on the activity, separate terms, privacy notices, disclosures or consents issued by Lympid, BMCP, the relevant issuer, the relevant white-label client and/or licensed partners may also apply.

## 2. Controller details

For the purposes of this Privacy Policy, the main controller for the processing activities described herein is:

LYMPID LABS, LDA, Avenida da Liberdade, no. 706, 2nd floor, 4710-249 Braga, Portugal, taxpayer number 517579499, email: [client.journey@lympid.io](mailto:client.journey@lympid.io), website: [lympid.io](https://lympid.io).

If you have any questions about this Privacy Policy or wish to exercise your data protection rights, you may contact us at [client.journey@lympid.io](mailto:client.journey@lympid.io).

### **3. Role allocation and relationship with other parties**

Because Lympid provides white-label infrastructure in a regulated and partner-based operating model, the data protection roles may vary depending on the activity being carried out.

As a general rule, Lympid, BMCP and/or the relevant licensed partners act as independent controllers for personal data processed for KYC/AML, sanctions screening, fraud prevention, onboarding, transaction monitoring, regulatory reporting, complaints handling, litigation, security logging and legally mandated record retention.

The relevant white-label client and/or issuer usually acts as an independent controller for its own product structuring, issuer relations, product-related investor communications, marketing, CRM, legal compliance and support activities outside Lympid's processor role.

To the extent Lympid processes personal data solely on behalf of a white-label client for purely client-instructed activities such as white-label operational tooling, registry administration or investor communications initiated by that client, Lympid may act as processor instead of controller.

Where required by the applicable operating model, you may be asked to enter into direct contractual relationships with Lympid, BMCP and/or one or more licensed partners, and to accept separate end-user terms, privacy notices, disclosures, payment terms, custody terms or consent language.

### **4. Personal data we may collect**

Depending on the product, journey and regulatory requirements, Lympid may collect and process the following categories of personal data:

- identification data, such as your full name, date of birth, nationality, tax identification details, tax residency and similar personal identifiers;
- contact details, such as your residential address, email address and telephone number;
- account and portal data, such as login credentials, account identifiers, investor category, account status and records of your interactions with the platform;
- onboarding and verification data, such as copies of identity documents, proof of address, questionnaire responses, source-of-funds or source-of-wealth information, PEP information, sanctions screening information, liveness or selfie checks, and other evidence required for due diligence;
- transaction and subscription data, such as subscription amounts, payment references, banking information, wallet addresses, blockchain transaction references, investment records and transfer or distribution history;

- appropriateness, suitability or categorisation data, where the applicable product flow or regulatory model requires investor categorisation or related assessment;
- documentation and execution data, such as electronically signed agreements, acceptance records, audit trails, timestamps and evidence of consent or acknowledgement;
- communications and support data, such as emails, portal messages, call notes, complaint files and support records;
- technical data, such as device identifiers, browser type, operating system, IP address, access timestamps, referral URLs, cookies, server logs and similar usage information; and
- marketing and preference data, including newsletter or communication preferences where marketing communications are enabled.

## **5. Sources of personal data**

We may obtain personal data directly from you, from the relevant white-label client or issuer, from BMCP, from licensed partners such as Tradevest GmbH, Sumsb and other onboarding, payment, custody, registry, execution, signature or compliance providers, from publicly available sanctions or PEP sources, from anti-fraud or verification databases, and from your use of the relevant website, application or portal.

## **6. Purposes of processing and legal bases**

Lympid may process personal data for the following purposes and on the following legal bases under the GDPR:

- to create and administer your account, provide access to the platform, operate investor journeys and perform pre-contractual steps or contractual obligations (Article 6(1)(b));
- to verify your identity, conduct KYC/AML, sanctions screening, source-of-funds checks, fraud prevention, transaction monitoring, regulatory reporting and legally required record retention (Article 6(1)(c) and, where relevant, Article 6(1)(f));
- to carry out investor categorisation, appropriateness or suitability related workflows where applicable to the relevant service or distribution model (Article 6(1)(b), Article 6(1)(c) and/or Article 6(1)(f));
- to facilitate subscriptions, payments, settlement support, custody arrangements, investor registry functions, digital execution, notices, lifecycle events and distributions (Article 6(1)(b), Article 6(1)(c) and/or Article 6(1)(f));
- to maintain platform integrity, detect misuse, secure systems, investigate incidents, enforce the Terms and Conditions and defend or establish legal claims (Article 6(1)(f) and, where relevant, Article 6(1)(c));
- to respond to your enquiries, complaints and support requests (Article 6(1)(b), Article 6(1)(c) and/or Article 6(1)(f));

- to send marketing communications or place non-essential cookies where consent is required by law (Article 6(1)(a)); and
- to comply with regulatory expectations, audit requests, court orders, competent authority requests and similar legal requirements (Article 6(1)(c)).

Where special categories of data are exceptionally involved, they will only be processed where a valid exemption under Article 9 GDPR applies and where such processing is necessary and proportionate under the relevant legal framework.

## **7. Automated checks and decision-making**

Lympid, BMCP and/or licensed partners may use automated tools in connection with identity verification, sanctions screening, fraud detection, transaction monitoring, risk scoring, onboarding routing and similar compliance controls.

These tools may contribute to decisions such as requesting additional information, delaying or refusing onboarding, restricting a transaction, escalating a case for manual review or terminating access where required by law, partner policy or prudent compliance practice.

Where required by applicable law, you may request human review of a decision, express your point of view and contest the decision by contacting us at [client.journey@lympid.io](mailto:client.journey@lympid.io).

## **8. Recipients of personal data**

Your personal data may be shared, where relevant and lawful, with the following categories of recipients:

- BMCP in its capacity as Lympid's principal and/or as a regulated distribution or structuring party where applicable;
- licensed partners and service providers, including Tradevest GmbH, Sumsuub, payment institutions, electronic money institutions, banks, custodians, digital asset custody providers, registry providers, digital-signature providers, hosting providers, security providers, analytics or communications providers and other specialised vendors engaged to support the service;
- the relevant white-label client, issuer, SPV, asset-originator or other product-side entities where required for the investor journey or the operation of the relevant product;
- professional advisers, auditors, insurers, financing sources or group entities on a need-to-know basis;
- courts, regulators, supervisory authorities, law enforcement authorities, tax authorities or other public authorities where disclosure is required or appropriate under applicable law; and
- potential purchasers, successors or reorganised entities in the event of a corporate transaction, subject to appropriate confidentiality and legal safeguards.

## **9. International transfers**

Personal data may be processed within the European Economic Area, the United Kingdom and other jurisdictions that provide an adequate level of protection, or may otherwise be transferred using a lawful transfer mechanism such as adequacy decisions, standard contractual clauses or other safeguards permitted under applicable data protection law.

Where a transfer is based on your consent or another exceptional derogation, that will be handled only where legally appropriate and proportionate to the relevant purpose.

## **10. Retention of personal data**

Lympid retains personal data only for as long as necessary for the purposes for which it was collected, including for the performance of the relevant service, investor support, dispute management, security and audit purposes.

Where legal or regulatory obligations apply, including AML/CFT, fraud-prevention, tax, accounting, financial-services, complaints-handling or litigation-preservation obligations, personal data may be retained for the legally required or reasonably necessary period even after your account is closed or your relationship with the platform ends.

When retention is no longer necessary, personal data will be deleted, anonymised or securely archived in accordance with our retention framework and applicable law.

## **11. Cookies and similar technologies**

The relevant websites and portals may use cookies and similar technologies. Cookies are small text files placed on your device through your browser.

We may use essential cookies required for access, security, session management and platform functionality, and we may also use functional, analytics or marketing technologies where enabled and lawful. Depending on the implementation, these may include tools or providers such as Google Analytics, Meta Pixel, HubSpot, Intercom/Crisp, Mixpanel, Hotjar or similar technologies.

Cookies may help us recognise repeat visits, maintain login sessions, improve the usability and security of the platform, understand how the interface is used and, where permitted, optimise content or communications.

You may disable or delete cookies through your browser settings at any time. However, disabling certain cookies may prevent some parts of the platform from functioning correctly. Where consent is required for non-essential cookies, those cookies will only be placed after the relevant consent has been obtained and may be withdrawn later.

## **12. Security**

Lympid implements technical and organisational measures designed to protect personal data against unauthorised or unlawful processing and against accidental loss, destruction, damage, alteration or disclosure.

These measures may include role-based access controls, encryption in transit and at rest where appropriate, backup and restoration procedures, vulnerability and patch management, incident-response procedures, business continuity planning, confidentiality commitments and staff security-awareness measures. No internet or electronic transmission system is entirely risk-free. You should also use appropriate personal security measures, including protecting your credentials, devices and email account.

### **13. Your rights**

Subject to applicable law and the circumstances of the relevant processing, you may have the right to request confirmation, access, rectification, erasure, restriction of processing, data portability and objection to processing, and to withdraw consent where processing is based on consent.

You also have the right to lodge a complaint with the competent supervisory authority, including the Portuguese data protection authority (CNPD) or the supervisory authority in your place of residence or work within the EEA, if you believe your data protection rights have been infringed.

To exercise any right, please contact [client.journey@lympid.io](mailto:client.journey@lympid.io). We may ask you to provide information necessary to verify your identity before responding to your request.

### **14. Third-party links and external environments**

The platform may contain links to third-party websites, wallets, payment pages, product pages, issuer pages or other external resources. Lymphid is not responsible for the content, security or privacy practices of third-party websites or services that are not controlled by Lymphid. You should review the relevant privacy notices and terms before using those services.

### **15. Changes to this Privacy Policy**

Lymphid may update this Privacy Policy from time to time to reflect changes in law, regulatory expectations, technology, services, operating model or data-processing practices.

The updated version will become effective when made available through the relevant website, portal or other appropriate communication channel, unless a different effective date is stated.

---

---

# **BMCP Privacy Policy**

## Privacy Policy

We are very delighted that you have shown interest in our enterprise. Data protection is of a particularly high priority for the management of BMCP GmbH. The use of the Internet pages of BMCP GmbH is possible without any indication of personal data; however, if a data subject wants to use special enterprise services via our website, processing of personal data could become necessary. If the processing of personal data is necessary and there is no statutory basis for such processing, we generally obtain consent from the data subject. The processing of personal data, such as the name, address, e-mail address, or telephone number of a data subject shall always be in line with the General Data Protection Regulation (GDPR), and in accordance with the country-specific data protection regulations applicable to BMCP GmbH. By means of this data protection declaration, our enterprise would like to inform the general public of the nature, scope, and purpose of the personal data we collect, use and process. Furthermore, data subjects are informed, by means of this data protection declaration, of the rights to which they are entitled. As the controller, BMCP GmbH has implemented numerous technical and organizational measures to ensure the most complete protection of personal data processed through this website. However, Internet-based data transmissions may in principle have security gaps, so absolute protection may not be guaranteed. For this reason, every data subject is free to transfer personal data to us via alternative means, e.g. by telephone.

### 1. Definitions

The data protection declaration of BMCP GmbH is based on the terms used by the European legislator for the adoption of the General Data Protection Regulation (GDPR). Our data

protection declaration should be legible and understandable for the general public, as well as

our customers and business partners. To ensure this, we would like to first explain the terminology used.

In this data protection declaration, we use, inter alia, the following terms:

**a) Personal data**

Personal data means 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.

**b) Data subject** Data subject is any identified or identifiable natural person, whose personal data is

processed by the controller responsible for the processing.

**c) Processing**

Processing is any operation or set of operations which is performed on personal data or on

sets of personal data, whether or not by automated means, such as collection, recording,

organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

**d) Restriction of processing**

Restriction of processing is the marking of stored personal data with the aim of limiting their

processing in the future.

**e) Profiling**

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.

**f) Pseudonymisation**

Pseudonymisation is the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

**g) Controller or controller responsible for the processing**

Controller or controller responsible for the processing is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

**h) Processor**

Processor is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

**i) Recipient**

Recipient is a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

**j) Third party**

Third party is a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

**k) Consent**

Consent of the data subject is any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear

affirmative action, signifies agreement to the processing of personal data relating to him or her.

## **2. Name and Address of the controller**

Controller for the purposes of the General Data Protection Regulation (GDPR), other data

protection laws applicable in Member states of the European Union and other provisions related to data protection is:

BMCP GmbH

Prannerstr. 10

80333 Munich

Germany

Email: [office@blackmanta.capital](mailto:office@blackmanta.capital)

Website: <https://blackmanta.capital/>

## **3. Cookies**

The Internet pages of BMCP GmbH use cookies. Cookies are text files that are stored in a

computer system via an Internet browser.

Many Internet sites and servers use cookies. Many cookies contain a so-called cookie ID. A

cookie ID is a unique identifier of the cookie. It consists of a character string through which

Internet pages and servers can be assigned to the specific Internet browser in which the cookie

was stored. This allows visited Internet sites and servers to differentiate the individual browser

of the data subject from other Internet browsers that contain other cookies. A specific Internet

browser can be recognized and identified using the unique cookie ID. Through the use of cookies, BMCP GmbH can provide the users of this website with more user-friendly services that would not be possible without the cookie setting.

By means of a cookie, the information and offers on our website can be optimized with the user

in mind. Cookies allow us, as previously mentioned, to recognize our website users.

The

purpose of this recognition is to make it easier for users to utilize our website. The website user

that uses cookies, e.g. does not have to enter access data each time the website is accessed, because this is taken over by the website, and the cookie is thus stored on the user's computer system. Another example is the cookie of a shopping cart in an online shop. The online store remembers the articles that a customer has placed in the virtual shopping cart via a cookie.

The data subject may, at any time, prevent the setting of cookies through our website by means of a corresponding setting of the Internet browser used, and may thus permanently deny the setting of cookies. Furthermore, already set cookies may be deleted at any time via an Internet browser or other software programs. This is possible in all popular Internet browsers. If the data subject deactivates the setting of cookies in the Internet browser used, not all functions of our website may be entirely usable.

#### **4. Collection of general data and information**

The website of BMCP GmbH collects a series of general data and information when a data subject or automated system calls up the website. This general data and information are stored in the server log files. Collected may be (1) the browser types and versions used, (2) the operating system used by the accessing system, (3) the website from which an accessing system reaches our website (so-called referrers), (4) the sub-websites, (5) the date and time of access to the Internet site, (6) an Internet protocol address (IP address), (7) the Internet service provider of the accessing system, and (8) any other similar data and information that may be used in the event of attacks on our information technology systems. When using these general data and information, BMCP GmbH does not draw any conclusions about the data subject. Rather, this information is needed to (1) deliver the content of our website correctly, (2) optimize the content of our website as well as its advertisement, (3)

ensure the long-term viability of our information technology systems and website technology,  
and (4) provide law enforcement authorities with the information necessary for criminal prosecution in case of a cyber-attack. Therefore, BMCP GmbH analyzes anonymously collected data and information statistically, with the aim of increasing the data protection and data security of our enterprise, and to ensure an optimal level of protection for the personal data we process. The anonymous data of the server log files are stored separately from all personal data provided by a data subject.

## **5. Contact possibility via the website**

The website of BMCP GmbH contains information that enables a quick electronic contact to our enterprise, as well as direct communication with us, which also includes a general address of the so-called electronic mail (e-mail address). If a data subject contacts the controller by e-mail or via a contact form, the personal data transmitted by the data subject are automatically stored. Such personal data transmitted on a voluntary basis by a data subject to the data controller are stored for the purpose of processing or contacting the data subject.

## **6. Routine erasure and blocking of personal data**

The data controller shall process and store the personal data of the data subject only for the period necessary to achieve the purpose of storage, or as far as this is granted by the European legislator or other legislators in laws or regulations to which the controller is subject to. If the storage purpose is not applicable, or if a storage period prescribed by the European legislator or another competent legislator expires, the personal data are routinely blocked or erased in accordance with legal requirements.

## **7. Rights of the data subject**

### **a) Right of confirmation**

Each data subject shall have the right granted by the European legislator to obtain from the

controller the confirmation as to whether or not personal data concerning him or her are being processed. If a data subject wishes to avail himself of this right of confirmation, he or

she may, at any time, contact any employee of the controller.

#### **b) Right of access**

Each data subject shall have the right granted by the European legislator to obtain from the

controller free information about his or her personal data stored at any time and a copy of

this information. Furthermore, the European directives and regulations grant the data subject access to the following information:

- the purposes of the processing;
- the categories of personal data concerned;
- the recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
- where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- the existence of the right to request from the controller rectification or erasure of personal data, or restriction of processing of personal data concerning the data subject, or to object to such processing;
- the existence of the right to lodge a complaint with a supervisory authority;
- where the personal data are not collected from the data subject, any available information as to their source;
- the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) of the GDPR and, at least in those cases, meaningful information about the logic involved, as well as the significance and envisaged consequences of such processing for the data subject. Furthermore, the data subject shall have a right to obtain information as to whether personal data are transferred to a third country or to an international organisation.

Where

this is the case, the data subject shall have the right to be informed of the appropriate safeguards relating to the transfer.

If a data subject wishes to avail himself of this right of access, he or she may, at any time,

contact any employee of the controller.

#### **c) Right to rectification**

Each data subject shall have the right granted by the European legislator to obtain from the

controller without undue delay the rectification of inaccurate personal data concerning him

or her. Taking into account the purposes of the processing, the data subject shall have the

right to have incomplete personal data completed, including by means of providing a supplementary statement.

If a data subject wishes to exercise this right to rectification, he or she may, at any time, contact any employee of the controller.

#### **d) Right to erasure (Right to be forgotten)**

Each data subject shall have the right granted by the European legislator to obtain from the

controller the erasure of personal data concerning him or her without undue delay, and the

controller shall have the obligation to erase personal data without undue delay where one of

the following grounds applies, as long as the processing is not necessary:

-The personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed.

-The data subject withdraws consent to which the processing is based according to point

(a) of Article 6(1) of the GDPR, or point (a) of Article 9(2) of the GDPR, and where there is no other legal ground for the processing.

-The data subject objects to the processing pursuant to Article 21(1) of the GDPR and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2) of the GDPR.

-The personal data have been unlawfully processed.

-The personal data must be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject.

-The personal data have been collected in relation to the offer of information society services referred to in Article 8(1) of the GDPR.

If one of the aforementioned reasons applies, and a data subject wishes to request the erasure of personal data stored by BMCP GmbH, he or she may, at any time, contact any

employee of the controller. An employee of BMCP GmbH shall promptly ensure that the erasure request is complied with immediately. Where the controller has made personal data public and is obliged pursuant to Article 17(1)

to erase the personal data, the controller, taking account of available technology and the cost

of implementation, shall take reasonable steps, including technical measures, to inform

other controllers processing the personal data that the data subject has requested erasure by

such controllers of any links to, or copy or replication of, those personal data, as far as processing is not required. Any employees of BMCP GmbH will arrange the necessary measures in individual cases.

#### **e) Right of restriction of processing**

Each data subject shall have the right granted by the European legislator to obtain from the

controller restriction of processing where one of the following applies:

-The accuracy of the personal data is contested by the data subject, for a period enabling

the controller to verify the accuracy of the personal data.

-The processing is unlawful and the data subject opposes the erasure of the personal data and requests instead the restriction of their use instead.

-The controller no longer needs the personal data for the purposes of the processing, but

they are required by the data subject for the establishment, exercise or defence of legal claims.

-The data subject has objected to processing pursuant to Article 21(1) of the GDPR pending the verification whether the legitimate grounds of the controller override those of the data subject.

If one of the aforementioned conditions is met, and a data subject wishes to request the restriction of the processing of personal data stored by BMCP GmbH, he or she may at any

time contact any employee of the controller. The employee of BMCP GmbH will arrange the

restriction of the processing.

#### **f) Right to data portability**

Each data subject shall have the right granted by the European legislator, to receive the personal data concerning him or her, which was provided to a controller, in a structured, commonly used and machine-readable format. He or she shall have the right to transmit those data to another controller without hindrance from the controller to which the personal

data have been provided, as long as the processing is based on consent pursuant to point (a)

of Article 6(1) of the GDPR or point (a) of Article 9(2) of the GDPR, or on a contract pursuant

to point (b) of Article 6(1) of the GDPR, and the processing is carried out by automated means, as long as the processing is not necessary for the performance of a task carried out in

the public interest or in the exercise of official authority vested in the controller. Furthermore, in exercising his or her right to data portability pursuant to Article 20(1) of the GDPR, the data subject shall have the right to have personal data transmitted directly from one controller to another, where technically feasible and when doing so does not adversely affect the rights and freedoms of others. In order to assert the right to data portability, the data subject may at any time contact any employee of BMCP GmbH.

**g) Right to object**

Each data subject shall have the right granted by the European legislator to object, on grounds relating to his or her particular situation, at any time, to processing of personal data concerning him or her, which is based on point (e) or (f) of Article 6(1) of the GDPR. This also applies to profiling based on these provisions.

BMCP GmbH shall no longer process the personal data in the event of the objection, unless we can demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject, or for the establishment, exercise or defence of legal claims.

If BMCP GmbH processes personal data for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing. This applies to profiling to the extent that it is related to such direct marketing. If the data subject objects to BMCP GmbH to the processing for direct marketing purposes, BMCP GmbH will no longer process the personal data for these purposes. In addition, the data subject has the right, on grounds relating to his or her particular situation, to object to processing of personal data concerning him or her by BMCP GmbH for scientific or historical research purposes, or for statistical purposes pursuant to Article 89(1) of the GDPR, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

In order to exercise the right to object, the data subject may contact any employee of BMCP

GmbH In addition, the data subject is free in the context of the use of information society

services, and notwithstanding Directive 2002/58/EC, to use his or her right to object by automated means using technical specifications.

#### **h) Automated individual decision-making, including profiling**

Each data subject shall have the right granted by the European legislator not to be subject to

a decision based solely on automated processing, including profiling, which produces legal

effects concerning him or her, or similarly significantly affects him or her, as long as the decision (1) is not necessary for entering into, or the performance of, a contract between

the data subject and a data controller, or (2) is not authorised by Union or Member State law

to which the controller is subject and which also lays down suitable measures to safeguard

the data subject's rights and freedoms and legitimate interests, or (3) is not based on the

data subject's explicit consent. If the decision (1) is necessary for entering into, or the performance of, a contract between

the data subject and a data controller, or (2) it is based on the data subject's explicit consent,

BMCP GmbH shall implement suitable measures to safeguard the data subject's rights and

freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and contest the decision.

If the data subject wishes to exercise the rights concerning automated individual decision-making, he or she may, at any time, contact any employee of BMCP GmbH.

#### **i) Right to withdraw data protection consent**

Each data subject shall have the right granted by the European legislator to withdraw his or

her consent to processing of his or her personal data at any time.

If the data subject wishes to exercise the right to withdraw the consent, he or she may, at

any time, contact any employee of BMCP GmbH.

## **8. Legal basis for the processing**

Art. 6(1) lit. a GDPR serves as the legal basis for processing operations for which we obtain consent for a specific processing purpose. If the processing of personal data is necessary for the performance of a contract to which the data subject is party, as is the case, for example, when processing operations are necessary for the supply of goods or to provide any other service, the processing is based on Article 6(1) lit. b GDPR. The same applies to such processing operations which are necessary for carrying out pre-contractual measures, for example in the case of inquiries concerning our products or services. Is our company subject to a legal obligation by which processing of personal data is required, such as for the fulfillment of tax obligations, the processing is based on Art. 6(1) lit. c GDPR. In rare cases, the processing of personal data may be necessary to protect the vital interests of the data subject or of another natural person. This would be the case, for example, if a visitor were injured in our company and his name, age, health insurance data or other vital information would have to be passed on to a doctor, hospital or other third party. Then the processing would be based on Art. 6(1) lit. d GDPR. Finally, processing operations could be based on Article 6(1) lit. f GDPR. This legal basis is used for processing operations which are not covered by any of the abovementioned legal grounds, if processing is necessary for the purposes of the legitimate interests pursued by our company or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data. Such processing operations are particularly permissible because they have been specifically mentioned by the European legislator. He considered that a legitimate interest could be assumed if the data subject is a client of the controller (Recital 47 Sentence 2 GDPR).

## **9. The legitimate interests pursued by the controller or by a third party**

Where the processing of personal data is based on Article 6(1) lit. f GDPR our legitimate interest is to carry out our business in favor of the well-being of all our employees and the shareholders.

#### **10. Period for which the personal data will be stored**

The criteria used to determine the period of storage of personal data is the respective statutory retention period. After expiration of that period, the corresponding data is routinely deleted, as long as it is no longer necessary for the fulfillment of the contract or the initiation of a contract.

#### **11. Provision of personal data as statutory or contractual requirement; Requirement necessary to enter into a contract; Obligation of the data subject to provide the personal data; possible consequences of failure to provide such data**

We clarify that the provision of personal data is partly required by law (e.g. tax regulations) or can also result from contractual provisions (e.g. information on the contractual partner). Sometimes it may be necessary to conclude a contract that the data subject provides us with personal data, which must subsequently be processed by us. The data subject is, for example, obliged to provide us with personal data when our company signs a contract with him or her. The non-provision of the personal data would have the consequence that the contract with the data subject could not be concluded. Before personal data is provided by the data subject, the data subject must contact any employee. The employee clarifies to the data subject whether the provision of the personal data is required by law or contract or is necessary for the conclusion of the contract, whether there is an obligation to provide the personal data and the consequences of non-provision of the personal data.

#### **12. Existence of automated decision-making**

As a responsible company, we do not use automatic decision-making or profiling.

### **13. Data transfer and use of third parties**

We will not pass on your personal data collected on the basis of your use of the website to third parties, unless it is necessary for the fulfillment of our obligations or mandatory by law. However, your personal data is also processed on our behalf by our service providers (**processors**). These processors are in particular marketing tool providers, IT service providers, providers of other tools and software solutions, IT maintenance services and other providers of similar services. All of our order processors process your data only on our behalf and on the basis of our instructions for our purposes outlined above.

#### **a) Data transfer**

A transfer of your personal data to other companies will only take place if:

- you have expressly given your consent to this in accordance with Art. 6 Para. 1 lit. a DSGVO or Art.49 Para. 1 lit. a
- the transfer according to Art. 6 Abs. 1 lit. f DSGVO for advertising or marketing purposes according to a publishing and direct marketing company (§151 GewO) is in our legitimate interest and there is no reason to believe that you have a superceding interest worthy of protection in the non-disclosure of your data. You have the possibility to object to our interest at any time and thus prevent the use of your data for direct marketing for the future.- in the event that there is a legal obligation for the disclosure in accordance with Art. 6 Para. 1 lit. c DSGVO
- the recipients are service providers who have a contract processing relationship with the controller under a contract pursuant to Art. 28 DSGVO.

#### **b) Data protection provisions on the use and application of. HubSpot**

We store and use contact data and information received (such as business communication histories) from customers and interested parties for the purpose of processing or initiating the business relationship. Personal data that you have communicated to us through a contact request (via website,

email, telephone, fax or in person), a newsletter registration or direct business relations are

processed and maintained by us with the help of a customer relationship management system (CRM system for short). We use applications from HubSpot as our customer database. Provider and order processor according to Art 28 DSGVO is HubSpot Germany

GmbH, Am Postbahnhof 17, 10243 Berlin (VAT: DE312070441). The data is stored on HubSpot's servers in the EU. Personal data processed within HubSpot are: Newsletters you

have subscribed to, contact details, projects for which you have shown interest. You have the

right to access the data stored about you in the customer database at any time and you can

request that the data be changed or deleted.

Further information on data protection under HubSpot CRM can be found online at:

<https://www.hubspot.com/data-privacy/gdpr>.

HubSpot is necessary for the proper operation of the website and funding. The legal basis

results from your consent according to Art 6 para 1 lit a or Art 6 para 1 lit b. if a contract is

concluded.

### **c) Data protection provisions regarding the use of a newsletter via HubSpot.**

We send newsletters, emails and other electronic notifications with promotional information

(hereinafter "newsletter") only with the consent of the recipients or a legal permission. Double opt-in and Storage. Registration for our newsletters take place in a so-called double opt-in process. This means that after registration you will receive an e-mail

in which you are asked to confirm your registration. This confirmation is necessary so that no

one can register with other e-mail addresses. The registrations for the newsletter are stored

in order to be able to prove the registration process according to the legal requirements.

This

includes the storage of the registration and confirmation time, as well as the IP address.

Changes to your data stored by HubSpot are also logged.

Use of the service provider "HubSpot" The newsletter is sent using "HubSpot Campaigns", a

service for newsletter dispatch from the provider HubSpot Germany GmbH, Am Postbahnhof

17, 10243 Berlin (VAT: DE312070441). The e-mail addresses of our newsletter recipients, as well as their other data described in the context of this notice, are stored on the servers of HubSpot in the Netherlands. HubSpot uses this information to send and evaluate the newsletters on our behalf. Furthermore, according to its own information, HubSpot may use this data to optimize or improve its own services, e.g. to technically optimize the dispatch and display of the newsletters or for economic purposes to determine from which countries the recipients come. However, HubSpot does not use the data of our newsletter recipients to address them itself or to pass them on to third parties. Furthermore, we have concluded a "Data Processing Agreement" with HubSpot. This is a contract in which HubSpot undertakes to protect the data of our users, to process it on our behalf in accordance with its data protection provisions and, in particular, not to pass it on to Third parties. You can view HubSpot's privacy policy here: <https://www.hubspot.com/data-privacy/gdpr>

Statistical collection and analyses: The newsletters contain a so-called "web beacon", i.e. a pixel-sized file that is retrieved from HubSpot's server when the newsletter is opened. Within the scope of this retrieval, technical information, such as information about the browser and your system, as well as your IP address and the time of the retrieval are initially collected. This information is used for the technical improvement of the services based on the technical data or the target groups and their reading behavior based on their retrieval locations (which can be determined with the help of the IP address) or the access times. The statistical surveys also include the determination of whether the newsletters are opened, when they are opened, and which links are clicked. For technical reasons, this information can be assigned to individual newsletter recipients. However, it is neither our intention nor that of

HubSpot to observe individual users. The evaluations serve us much more to recognize the reading habits of our users and to adapt our content to them or to send different content according to the interests of our users. Online call and data management  
There are cases where we direct newsletter recipients to HubSpot's websites. For example, our newsletters contain a link that newsletter recipients can use to access the newsletters online (e.g., in case of display problems in the email program). Furthermore, newsletter recipients can subsequently correct their data, such as the e-mail address. In this context, we point out that cookies are used on HubSpot's websites and that personal data is processed by HubSpot, its partners and service providers (e.g. Google Analytics). We have no influence on this data collection. For more information, please refer to HubSpot's privacy policy. We

would also like to draw your attention to the options for objecting to the collection of data for advertising purposes on the websites <http://www.aboutads.info/choices/> and <http://www.youronlinechoices.com/> (for the European region).

Cancellation/revocation: You can cancel the receipt of our newsletter at any time, i.e. revoke

your consents. This will simultaneously terminate your consents to its dispatch via HubSpot

and the statistical analyses. Unfortunately, a separate revocation of the dispatch via HubSpot

or the statistical analysis is not possible. You will find a link to cancel the newsletter at the

end of each newsletter.

#### **d) Privacy policy on the use and application of Youtube.**

This website uses a plugin of the video portal YouTube. The operator of the website is Google

Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland.

If you agree to the use, the video will be played directly from the Youtube server. In doing so,

the Youtube server is informed from which page you have accessed the video and from which IP address. If you are logged into Youtube as a user, this call is linked to your Youtube

profile. The USA is certified by the EU Court of Justice as having a low level of data

protection. If you give your consent according to Art 49 para 1 lit a, you expose yourself to the risk that your data will be viewed by the American government. To protect your data, the EU standard contractual clauses have been signed with the provider. This consent can be revoked at any time on this page.

Furthermore, YouTube may store various cookies on your terminal device or use comparable technologies for recognition (e.g. device fingerprinting). In this way, YouTube can obtain information about visitors to this website. This information is used, among other things, to collect video statistics, improve the user experience, and prevent fraud attempts. For more information on how we handle user data, please see YouTube's privacy policy at:

<https://policies.google.com/privacy?hl=de>.

#### **e) Privacy policy on the use and application of Instagram.**

The responsible party has integrated components of the service Instagram on this website.

Instagram is a service that qualifies as an audiovisual platform and allows users to share

photos and videos and also to redistribute such data in other social networks.

The operating company of the Instagram services is Instagram LLC, 1 Hacker Way, Building 14

First Floor, Menlo Park, CA, USA.

Each time one of the individual pages of this website operated by the responsible party is

called up and on which an Instagram component (Insta button) has been integrated, the internet browser on the information technology system of the data subject is automatically

caused by the respective Instagram component to download a representation of the corresponding component from Instagram. Within the scope of this technical procedure, Instagram receives knowledge about which specific subpage of our website is visited by the

data subject.

If the data subject is logged into Instagram at the same time, Instagram recognizes which

specific sub-page the data subject is visiting with each call to our website by the data subject

and for the entire duration of the respective stay on our website. This information is

collected by the Instagram component and assigned by Instagram to the respective Instagram account of the data subject. If the data subject activates one of the Instagram buttons integrated on our website, the data and information thus transmitted will be assigned to the personal Instagram user account of the data subject and stored and processed by Instagram.

Instagram always receives information via the Instagram component that the data subject

has visited our website if the data subject is simultaneously logged into Instagram at the time

of using our website; this takes place regardless of whether the data subject clicks on the

Instagram component or not. If the data subject does not want this information to be transmitted to Instagram, he or she can prevent the transmission by logging out of his or her

Instagram account before accessing our website.

The USA is certified by the EU Court of Justice as having a low level of data protection.

If you

give your consent in accordance with Art 49 para 1 lit a, you expose yourself to the risk that

your data will be viewed by the U.S. government. EU standard contractual clauses have been

signed with the provider to safeguard your data. This consent can be revoked at any time on

this page.

The applicable privacy policy of LinkedIn is available at:

<https://www.linkedin.com/legal/privacy-policy>.

LinkedIn's cookie policy is available at <https://www.linkedin.com/legal/cookie-policy>.

Further information and the applicable privacy policy of Instagram can be found at

<https://help.instagram.com/155833707900388>

and

<https://www.instagram.com/about/legal/privacy/>.

#### **f) Privacy policy on the use and application of LinkedIn.**

The responsible party has integrated components of the LinkedIn Corporation on this website. LinkedIn is an Internet-based social network that enables users to network with existing business contacts and to make new business contacts. Over 400 million registered

people use LinkedIn in more than 200 countries. This makes LinkedIn currently the largest

platform for business contacts and one of the most visited websites in the world.

The operating company of LinkedIn is LinkedIn Corporation, 2029 Stierlin Court Mountain View, CA 94043, USA. For data protection issues outside the USA, LinkedIn Ireland, Privacy Policy Issues, Wilton Plaza, Wilton Place, Dublin 2, Ireland, is responsible. With each individual usage of our website that is equipped with a LinkedIn component (LinkedIn plug-in), this component causes the browser used by the data subject to download a corresponding representation of the component from LinkedIn. Further information on LinkedIn plug-ins can be found at <https://developer.linkedin.com/plugins>. As part of this technical procedure, LinkedIn receives knowledge of which specific subpage of our website is visited by the data subject. If the data subject is logged in to LinkedIn at the same time, LinkedIn recognizes which specific sub-page of our website the data subject is visiting with each call-up of our website by the data subject and for the entire duration of the respective stay on our website. This information is collected by the LinkedIn component and assigned by LinkedIn to the respective LinkedIn account of the data subject. If the data subject activates a LinkedIn button integrated on our website, LinkedIn assigns this information to the personal LinkedIn user account of the data subject and stores this personal data. LinkedIn always receives information via the LinkedIn component that the data subject has visited our website if the data subject is simultaneously logged into LinkedIn at the time of calling up our website; this takes place regardless of whether the data subject clicks on the LinkedIn component or not. If the data subject does not want this information to be transmitted to LinkedIn, he or she can prevent the transmission by logging out of his or her LinkedIn account before accessing our website. The USA is certified by the EU Court of Justice as having a low level of data protection. If you give your consent in accordance with Art 49 para 1 lit a, you expose yourself to the risk that your data will be viewed by the American government. To protect your data, the EU standard contractual clauses have been signed with the provider. This consent can be revoked at any

time on this page.

The applicable privacy policy of LinkedIn is available at:

<https://www.linkedin.com/legal/privacy-policy>.

LinkedIn's cookie policy is available at <https://www.linkedin.com/legal/cookie-policy>.

### **g) Privacy policy on the use and application of Twitter**

The responsible party has integrated components of Twitter on this website. Twitter is a multilingual publicly accessible microblogging service on which users can publish and distribute so-called tweets, i.e. short messages that are limited to 280 characters. These short messages can be accessed by anyone, including people who are not registered with

Twitter. However, the tweets are also displayed to the so-called followers of the respective

user. Followers are other Twitter users who follow the tweets of a user. Furthermore, Twitter

makes it possible to address a broad audience via hashtags, links or retweets.

The operating company of Twitter is Twitter, Inc., 1355 Market Street, Suite 900, San Francisco, CA 94103, USA.

Each time one of the individual pages of this website operated by the responsible party is

used and on which a Twitter component (Twitter button) has been integrated, the Internet

browser on the information technology system of the data subject is automatically caused by

the respective Twitter component to download a representation of the corresponding Twitter component from Twitter. Further information on the Twitter buttons can be found at

<https://about.twitter.com/de/resources/buttons>. Within the scope of this technical procedure, Twitter receives knowledge of which specific sub-page of our website is visited by the data subject. The purpose of integrating the Twitter component is to enable our users to

disseminate the content of this website, to make this website known in the digital world and

to increase our visitor numbers.

If the data subject is logged into Twitter at the same time, Twitter recognizes which specific

subpage of our website the data subject is visiting each time the data subject uses our website and for the entire duration of the respective stay on our website. This information is

collected by the Twitter component and assigned by Twitter to the respective Twitter account of the data subject. If the data subject activates one of the Twitter buttons

integrated on our website, the data and information thus transmitted will be assigned to the personal Twitter user account of the data subject and stored and processed by Twitter. Twitter always receives information via the Twitter component that the data subject has visited our website if the data subject is simultaneously logged into Twitter at the time of calling up our website; this takes place regardless of whether the data subject clicks on the Twitter component or not. If the data subject does not want this information to be transmitted to Twitter, he or she can prevent the transmission by logging out of his or her Twitter account before accessing our website.

The USA is certified by the EU Court of Justice as having a low level of data protection. If you give your consent in accordance with Art 49 para 1 lit a, you expose yourself to the risk that your data may be viewed by the American government. To protect your data, the EU standard contractual clauses have been signed with the provider. This consent can be revoked at any time on this page.

The applicable data protection provisions of Twitter are available at:  
<https://twitter.com/privacy?lang=de>.

#### **h) Privacy policy on the use of Google Maps**

On our website, we use Google Maps to display map information. The operating company of the Google Maps component is Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland. In doing so, Google also processes data on the use of the Maps functions by visitors to the website and extracts this data in accordance with its privacy policy, which you can find at <https://www.google.at/intl/de/policies/privacy/>.

Access to data collected when using Google Maps by Google Inc. in the USA cannot be ruled out. The USA has been certified by the EU Court of Justice as having a low level of data protection. If you give your consent in accordance with Art 49 (1) lit a, you expose yourself to the risk that your data may be viewed by the American government. To protect your data, the EU standard contractual clauses have been signed with the provider. This consent can be revoked at any time on this page.

#### **i) Typeform**

We store and use contact data and information (such as business communication histories)

received from customers and prospective customers for the purpose of processing or initiating the business relationship.

Personal data that you provide to us by filling out a Typeform form (such as investment experience, email, phone and other personal information) is processed and maintained by us

using a customer relationship system.

Typeform's privacy policy can be found at the following link: <https://www.typeform.com>

#### **j) AWS - Amazon Web Services**

We use Amazon Web Services hosting to operate our website. This allows Amazon to automatically access all data stored via the hosting. This includes personal customer data -

such as names, addresses, email addresses, IP addresses and telephone numbers.

AWS's privacy policy can be found at the following link:

<https://aws.amazon.com/de/compliance/gdpr-center/>

#### **k) IDnow**

We use the KYC&AML provider IDnow to comply with regulatory requirements at European

and national level. In doing so, the service provider can access all requested information such

as personal customer data - such as names, addresses, email addresses, IP addresses, home

address, date of birth, source of funds, and telephone numbers.

IDnow's privacy policy can be found at the following link:

<https://www.idnow.io/de/datenschutzerklaerung/>

#### **l) SumSub**

We use the KYC&AML provider SumSub to comply with the regulatory requirements on European and national level. In doing so, the service provider can access all requested information such as personal customer data - such as names, addresses, email

addresses, IP

addresses, home address, date of birth, source of funds, and telephone numbers.

SumSub's privacy policy can be found at the following link:

<https://sumsub.com/privacy-notice-service/>

#### **m) Privacy policy on the use and application of Google Analytics (with anonymization**

**function)**The responsible party has integrated the Google Analytics component (with anonymization

function) on this website. Google Analytics is a web analysis service. Web analysis is the

collection, compilation and evaluation of data about the behavior of visitors to websites.

A

web analysis service collects, among other things, data on which website a data subject came to a website from (so-called referrers), which subpages of the website were accessed

or how often and for how long a subpage was viewed. A web analysis is mainly used for the

optimization of a website and for the cost-benefit analysis of internet advertising.

The operating company of the Google Analytics component is Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland.

The responsible party uses the addition "\_gat.\_anonymizeIp" for web analysis via Google

Analytics. By means of this additive, the IP address of the Internet connection of the data

subject is shortened and anonymized by Google if access to our Internet pages is from a

member state of the European Union or from another state party to the Agreement on the

European Economic Area.

The purpose of the Google Analytics component is to analyze the flow of visitors to our website. Google uses the data and information obtained, among other things, to evaluate

the use of our website, to compile online reports for us showing the activities on our website, and to provide other services related to the use of our website.

Google Analytics sets a cookie on the information technology system of the data subject.

What cookies are has already been explained above. By setting the cookie, Google is enabled

to analyze the use of our website. By each call of one of the individual pages of this website,

which is operated by the responsible person and on which a Google Analytics component has

been integrated, the internet browser on the information technology system of the data subject is automatically caused by the respective Google Analytics component to transmit

data to Google for the purpose of online analysis. As part of this technical process, Google

obtains knowledge of personal data, such as the IP address of the data subject, which Google

uses, among other things, to track the origin of visitors and clicks and subsequently enable commission calculations.

Through the use of the cookie, personal information, such as the access time, the location from which an access originated and the frequency of visits to our website by the data subject, is stored. Each time the data subject visits our website, this personal data, including

the IP address of the internet connection used by the data subject, is transmitted to Google

in the United States of America. This personal data is stored by Google in the United States of

America. The USA is certified by the EU-CJ as having a low level of data protection. If you give

your consent in accordance with Art 49 para 1 lit a, you expose yourself to the risk that your

data will be viewed by the American government. To secure your data, the EU standard contractual clauses have been signed with the provider. This consent can be revoked at any

time on this page. Further information and the applicable Google privacy policy can be found at

<https://www.google.de/intl/de/policies/privacy/>

And at

<http://www.google.com/analytics/terms/de.html>.

Google Analytics is explained in more detail under this link:

[www.google.com/intl/de\\_de/analytics/](http://www.google.com/intl/de_de/analytics/).

#### **n) LINKS**

Our platform may contain links to other websites on the Internet. We are not responsible for

the content of those websites or for any other privacy practices on those websites. You should read the terms of use and privacy statements of each website you link to from our

website that collects information over the Internet. Our Terms of Use and Privacy Policy apply only to information we collect in accordance with this policy. If you become aware of

any misuse or inappropriate content on a website to which we link, please notify us so that

we may take actions as soon as possible.