

AML and CTF Information and Personal Data Processing Notice

Safeguard World International Ltd. ("Safeguard Global", "we", "us") provides you with this Information Notice in order to allow you to understand our policy regarding your privacy. As such, this Information Notice explains how Safeguard Global handles your personal data for anti-money laundering ("AML") and counter-terrorist financing ("CTF") purposes as part of our Know Your Client ("KYC") activities.

In general, any information which you provide us will be processed in a lawful, fair, and transparent manner. To this end, Safeguard Global acts according to internationally recognized principles with regards to the processing of personal data, such as purpose limitation, storage limitation, data minimization, and confidentiality.

Please note that, at the end of this document, you will find "Definitions", referring to more detailed explanations of the underlined terms.

1. Data Controller and Data Protection Officer

Safeguard World International Ltd., with registered office in Ground Floor, Building 2 Campion Park, Holmes Chapel, Crewe, Cheshire, England, CW4 8AX is the data controller regarding the processing of personal data carried out for AML and CTF purposes.

If, after reading this Information Notice, you have any further questions regarding how we may use your personal data, please contact: privacy@safeguardglobal.com.

If you would like to speak or get in touch with our Data Protection Officer (DPO) for any queries or content in this Information Notice, please contact: dpo@safeguardglobal.com.

2. Personal Data Processed

a. Personal Data you provide.

In the context of its KYC activities, Safeguard Global collects personal data that is necessary for AML / CTF purposes and the other purposes identified in section 4 below ("*4. Purposes of processing and grounds for processing*"). To this aim, Safeguard Global collects the information listed below pertaining to the Ultimate Beneficial Owner and to other individuals which are otherwise connected with Safeguard Global's clients and / or prospective clients, such as personal data pertaining to directors, officers, authorized representatives, and family members of the above-mentioned individuals.

In particular, Safeguard Global collects the name and surname of the legal representative of the company concerned, of the majority shareholder and of the Ultimate Beneficial Owner in order to identify those individuals.

Additional information is collected in relation to the Ultimate Beneficial Owner (or, in case there is no natural person as Ultimate Beneficial Owner, the Chairman/CEO/Managing Director or a person with similar roles and responsibilities of the company), such as: email address, residential and work address, telephone number, national identification number or passport number, date and country of birth, nationality, profession / job title, other employment details (e.g., professional qualifications and / or memberships), annual income, and details of shareholdings in the company.

In order to comply with the specific requirements under the AML / CTF laws and regulations to which Safeguard Global is subject, the following information is collected in addition to those listed above: whether the Ultimate Beneficial Owner is a politically exposed person (and, if so, the related title / profession and time period of such title) and / or whether the Ultimate Beneficial Owner has a close relationship with an individual which is a politically exposed person (and, if so, name, surname, national identification number or passport number, title / profession and time period of such title and the level of association of the Ultimate Beneficial Owner with such individual).

As a proof of the information provided, we also collect the following documents: copy of identity documents (e.g., passport, identity card, residence permit), copy of bank notices / statements, copy of utility bill / residence lease contract, copy of employment certificate and of social security certificate, and copy of a recent pay slip, copy of phone bill.

b. Personal Data collected from public sources / third-party services

In addition to the above, we may also process any additional personal data that we may be able to collect when carrying out checks from public sources and / or from third-party services that we use for verification purposes and to collect additional insights and information on the company concerned.

c. Other person's personal data

Please consider that if you provide personal data of third parties, you are responsible for ensuring that you have the necessary consent or other legal justification to do so and that you assume all other applicable obligations and responsibilities prescribed by the law, including the obligation to inform those individuals that their personal data is shared with Safeguard Global and processed for the purposes described in this Information Notice.

3. Sources of Personal Data

We may receive personal data about you:

- directly from you;
- your employer (and / or from the company you are otherwise affiliated with);
- publicly available resources;
- trusted third-party databases that we use for verification purposes.

4. Purposes of processing and grounds for processing

Safeguard Global processes personal data for the purpose of:

- a. Complying with AML and CTF laws and regulations;
- b. Responding to and complying with any other legal / regulatory requirements to which Safeguard Global is subject and / or disclosure requests or other orders from public authorities.

The processing activities performed for the purposes identified in points a) and b) above are lawful as they are mandated by the applicable laws / regulations / court or regulatory orders to which Safeguard Global is subject.

- c. Protecting our interests and those of other parties in the context of the establishment, exercise or defense of legal claims that may be brought by or against Safeguard Global as well as in out-of-court and pre-litigation phases.

The processing activities performed for the purposes identified in point c) above are lawful as they respond to Safeguard Global's legitimate interest in defending its interests and those of third parties.

The provision of personal data for the above mentioned purposes (a), b) and c)) is mandatory with the result that the refusal to provide personal data for such purposes will prevent Safeguard Global from entering into a business relationship with you / the company you represent.

5. Recipients of Personal Data

The personal data collected in the context of the above-mentioned activities may be transmitted to the following categories of individuals / entities (hereinafter, "Recipients"):

- persons authorised by Safeguard Global to process personal data, who have undertaken an obligation of confidentiality or are subject to an appropriate legal obligation of confidentiality (e.g., employees of Safeguard Global);
- consultants as well as other third-parties and suppliers which may be engaged for administrative, legal and technical maintenance purposes;
- public authorities, bodies or entities to which personal data may need to be disclosed under the applicable law or binding orders from competent authorities;
- other companies within the Safeguard Global group as needed in order to achieve the purposes listed in this Information Notice.

6. Transfer of Personal Data

Considering Safeguard Global's worldwide presence and business operations, personal data may be transferred to Recipients located in several different countries. Transfers of your personal data to Recipients may be based on an adequacy decision, the Standards Contractual Clauses approved by the European Commission or any other lawful transfer mechanism. More information is available by writing to privacy@safeguardglobal.com.

7. Retention of Personal Data

Your personal data will be kept for the time necessary in order to comply with the applicable legal and regulatory requirements and for the time needed in order to protect our interests and those of third parties in the event of legal claims / other contentious or pre-contentious situations.

In particular, personal data that have been collected for KYC purposes are kept for a period of **five (5) years** after the end of the business relationship with Safeguard Global's client. At the end of this timeframe, Safeguard Global will delete the personal data, unless their retention for a longer period of time, which may not exceed ten (10) years, is permitted or required by legal or regulatory applicable provisions.

Further information on retention periods is available, upon request at: privacy@safeguardglobal.com.

8. Data subject's rights

As a data subject, you are entitled to exercise the following rights before Safeguard Global (where applicable):

- Access your personal data: you have the right to receive the personal data we hold about you as well as information on the processing of your personal data;
- Correct or update your personal data: you have the right to ask us to rectify your personal data where it is inaccurate or incomplete;
- Request erasure of your personal data: you have the right to request the deletion of your personal data, where you feel that the processing is unnecessary or otherwise unlawful (unless there are other reasons that justify a further retention of your personal data);
- Request the restriction of the processing of your personal data: you have the right to request the restriction of the processing of your personal data, where you feel that the personal data processed is inaccurate, unnecessary or unlawfully processed, or where you have objected to the processing;
- Exercise your right to portability: you have the right to obtain a copy of your personal data provided to Safeguard Global, in a structured, commonly used and machine-readable format, and you may also request the transmission of that personal data to another data controller;
- Object to the processing of your personal data: you have the right to request that we stop / cease the processing of your personal data, where applicable, on the basis of relevant grounds related to your particular situation, which you believe must prevent Safeguard Global from processing your personal data; or
- Withdraw your consent to processing, where your consent serves as the legal basis for processing (this will not affect the lawfulness of processing carried out prior to your withdrawal).

Requests to exercise any of the above rights must be sent in writing to us at the following address: privacy@safeguardglobal.com.

At any time, you can also:

- Contact our Data Protection Officer (DPO) by writing to dpo@safeguardglobal.com.
- Contact the competent Supervisory Authority (in the Member State of your habitual residence, place of work or place of the alleged infringement) whose contact details are available [here](#) (for UK click [here](#)), if you believe that the processing of your personal data carried out by Safeguard Global is unlawful.

9. Definitions

Data controller: refers to the legal person, public authority, service or other entity which, individually or jointly, determines the purposes and means for processing your personal data.

Data minimization: the principle of “data minimization” provides that personal data shall be “adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed”. This means that the data controller must only collect the least amount of personal data that it needs to achieve its purposes.

Personal data: any information concerning an identified or identifiable data subject. A data subject considered identifiable is one who can be identified, directly or indirectly, by an identifier such as a name, an identification number, location data, an online identifier or by one or more factors specific to their physical, physiological, genetic, mental, economic, cultural or social identity.

Processing: refers to any operation or set of operations carried out on personal data or on sets of personal data, by automated or other means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Purpose limitation: the principle of “purpose limitation” provides that personal data shall be “collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes”. This means that the purposes for processing personal data should be clearly defined by the data controller before collecting personal data and that the processing activities should be clearly monitored by the data controller in order to ensure that personal data are only processed for the purposes for which they have been collected.

Storage limitation: the principle of “storage limitation” provides that personal data shall be “kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed”. This means that personal data shall not be kept by the data controller for longer than needed and that time limits should be set up for erasure or periodic review.