Privacy Policy for Data Subjects

SGR Compliance SA, Switzerland ("**SGR**", "**we**", "**us**", "**our**") produces and maintains several databases (specific collection of data) that are archives of publicly available information ordered according to different area of risk. The contents of the databases are available only to public authorities and public or private firms under the legal obligation to carry-out anti-money laundering, anti-terrorism financing ("**AML**" and "**CFT**") and Know Your Customer ("**KYC**") screenings. Please note that SGR does not conduct any personal investigative or factfinding activity or give any indication, assessment or score to any record we hold. International and domestic law globally are quite clear by imposing on specific activities, such as banks, financial intermediaries, fiduciaries and specific categories of businesses enhanced screening obligations to prevent the misuse of financial or professional services.

This Privacy Policy is addressed to data subjects ("**Data Subject**", "**you**", "**your**") whose personal information is contained in SGR databases (all together "**Database**").

This Privacy Policy explains how SGR collects, processes, discloses, stores and protects information about you in the context of our Database. It also provides information about your rights and about how you can contact us if you have questions about how we handle your information.

This Privacy Policy is based on the "*Bundesgesetz über den Datenschutz*" 1992 as amended ("**DSG**") [Swiss Federal Act on data protection] https://www.fedlex.admin.ch/eli/cc/1993/1945_1945_1945/de. SGR is authorized to treat and process personal data pursuant to those laws and regulations and by the Swiss *Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter* ("**EDÖB**") [Swiss Federal data protection and information commissioner]. Although the GDPR is a regulation of the European Union, it is of relevance to us. Furthermore, this Privacy Policy is also based on the General Data Protection Regulation (Regulation EU 2016/679) as amended ("**GDPR**"), in particular on its UK implementation of the GDPR UK "*Data Protection Act*" 2018 ("**DPA**") as amended https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.
Our European Representative and Data Protection Officer ("**DPO**") is Moore ClearComm, Devonshire House, 60 Goswell Road, London, EC1M 7AD, UK, dpo@sgrcompliance.com.
In this document we shall refer to the above mentioned DSG, and GDPR as implemented by DPA definitions and rules.

Content of this Privacy Policy

This Privacy Policy only refers to our Databases. For general information about privacy, please refer to our Privacy Policy for Website Users published on this website**.**

Purposes of the processing

SGR Databases process information in the public interest as defined and explained pursuant to DSG, GDPR and DPA provisions, since such information allows SGR customers (or prospects under free trial) (collectively "**Customers**") to better fulfil their legal obligations related to AML/CFT, KYC and due diligence requirements, to prevent and protect themselves against bribery/fraud/corruption and other unlawful acts, to lower the risk of misuse of professional or financial services and to verify monetary transactions to detect suspicious money flows (all together, "**Checks**"). SGR Customers are Regulated entities such as banks, insurances, asset managers, listed companies, public notaries, law firms, accountancy firms or other subjects/firms/entities obliged pursuant to AML, CTF, KYC to perform screening activities in accordance with their regulatory obligations and risk management procedures carried out in both their legitimate interest and in the public interest ("**Regulated Entities**" or "**RE**").

SGR offers a preliminary instrument to perform Checks, however Customers must carry out additional searches against names of their prospects, clients or counterparties, in order to verify, enhance or supplement their Checks. Should a Customer find information about you in SGR Database, this does not mean that either the person named in the article is actually you or that everything contained in publicly accessible data is accurate, complete, updated or correct. Customers are obliged to take further steps to verify the identity, interpretate the information and to determine how to use it. We inform our Customers that they cannot rely solely upon personal data and information found on SGR Database, but they must perform independent Checks and double check the identity and the accuracy of the personal data we collect and decide discretionary for themselves whether to conduct business with the individual or the entity they are verifying.

The inclusion of information about you on SGR Database does neither prevent RE from doing business with you nor should automatically be taken by the RE to draw any particular inference (negative or otherwise) about you. Customers are and shall remain solely responsible for verifying the suitability of the data provided by SGR and for adequately analysing the information for the purposes pursued in relation to the professional use for which it is intended, compliantly with the rules and regulations governing AML and CFT and with the applicable privacy rules and regulations in force.

The fact that RE make use of our Database does not exempt them from ensuring the accuracy of personal data they process, so that this must be verified with their prospects, clients or counterparties before any action is taken by the RE. SGR shall in no way be liable for the discretionary decisions or assessments made by the Customer based on the information contained in the Database. RE are also obliged to verify multiple sources of information, such us declaration of their prospects, clients or counterparties, internet information, newspapers or media. Customers undertake to use the Database only to accomplish AML and CFT regulations, to keep access credentials safe, guaranteeing their confidentiality and preventing them from being used improperly, being the Customer solely responsible for any use and decision thereof.

From which source the personal data originate - publicly accessible sources

Your information is included on SGR Database only if it is a publicly accessible data, found in publicly available, official or reliable/reputable or authoritative sources which are relevant for Checks [1]. Special care has been taken in the selection of the sources. We put our best effort to monitor the public available sources and ensure that information we hold about you is accurate, updated, relevant and not excessive, however, the correctness, completeness and update of our information depends on the correctness, completeness and update of the source of information and its constant publicly accessible nature.

[1] This means personal information available to the general public and usually over the internet, for instance found on: (i) sanction or watch lists available on public authorities websites; (ii) legal enforcement, court, regulatory actions found on government websites; (iii) political websites and publications such as parliamentary, local government or individual politician websites; (iv) reputable news media and publications; (v) public registers, lists, deeds or documents that are knowable by anyone; (vi) websites of public, governmental, territorial and local bodies, public agencies, as well as supervisory and control authorities and (vii) websites of trade associations and professional orders, with regard to lists or registers of economic and business operators, published on their own website; (viii) information made public by an individual themselves such as on social media, personal website or blog, biographical sources; (ix) data provided under open government licence.

Legal basis for the processing of information – public and legitimate interest

The lawful bases for SGR processing personal data, including special category of personal data relating to criminal convictions and offences, are set out in particular under: Article 31 of the DSG; Articles 6, 9 and 10 of the GDPR; Articles 8, 10, 11 and Schedule 1 of the DPA.
At least one of these must apply whenever personal data is to be processed:

a) Consent: you have given SGR your freely, specific, informed or unambiguous consent for your personal data to be processed for a specific purpose or, pursuant to Article 30.3 of the DSG and Schedule 1 of the DPA, "*this condition is met if the processing relates to personal data which is manifestly made public by the Data Subject*".
b) Contract performance: the processing is necessary for the performance of a contract you have with SGR, which had asked you to take specific steps before entering a contract.
c) Compliance with legal obligation: the processing is necessary for SGR to comply with the law in the jurisdictions where SGR operates (not including contractual obligations).
d) Protection of vital interests: the processing is vital to an individual's survival.
e) Public interest: the processing is necessary to perform a task that is in the public interest or for its official functions, and the task or function has a clear basis in law, so pursuant to Schedule 1 of the DPA this means "*preventing or detecting unlawful acts*", "*necessary for the purposes of preventing fraud or a particular kind of fraud*", "*regulatory requirements relating to unlawful acts and dishonesty*" and "*suspicion of terrorist financing or money laundering*". With reference to the production and maintenance of its Database, SGR falls into this scope and is authorized pursuant to Article 31 of the DSG, GDPR and DPA, laying the legal basis for the processing of personal data down by such Union Law and Member State law to which SGR is subject.
f) Legitimate interests: the processing is necessary for SGR's legitimate interests, or the legitimate interests of a third-party, including SGR Customers, unless there is a good reason to protect the individual's personal data that overrides those legitimate interests.

As mentioned, because the RE has a specific duty to screen their clients' database and collect information about existing client, prospect or counterpart to:

- verify the source of funds or to assess the purpose and the risk of the business relation;
- prevent and detect financial crime, corruption, fraud and serious misconduct or dishonesty;
- check the person to whom a business operation is directed;
- check a person associated or involved in a business operation with the client or prospect;
- check people involved in dubious economic transactions;
- combating ML/FT and protect the national security;
- reduce their risk and maintain their reputation;

and because this duty is set out by AML/CFT legislation enacted at a worldwide level, the SGR and RE have a legitimate interest in processing personal data.

Categories of personal data processed

Your information is typically included on SGR Database if a publicly accessible data indicates that:

- You are a "Politically Exposed Person" ("**PEP**"[2]) or other individual potentially subject to corruption risk (for instance, who has a relevant role in public administrations, is a local politician or is involved in public

[2] PEP: as indicated by FATF, persons who are or have been entrusted with prominent public functions so that are exposed to the possibility of corruption or the abuse of their position to a certain degree, those holding senior, prominent or important positions, with substantial authority over policy, operations or the use or allocation of government-owned resources.

procurement) as defined by the Financial Action Task Force recommendations ("**FATF**" or "**GAFI**") or European or National legislation. SGR records at least one source for every single PEP in the Database;

- You are a close associate or relative of a PEP, as defined by FATF or European or National legislation;
- You are a politician at a local level, which comprises all the municipalities, metropolitan cities, provinces and regions;
- You are listed or warned by a public financial authority, regulator, law enforcement authority or governmental body in connection with money-laundering, terrorist financing, bribery, corruption or similar activities;
- You are included on financial institutions and regulatory authorities' sanctions lists or watchlists, such as the UN, the European Union and OFAC (the Office of Foreign Assets Control of the US Treasury Department);
- You have been for instance accused, investigated, arrested, charged, convicted or allegedly involved in crimes/offences/proceedings for an offence committed or alleged which are connected, or are a possible pre-cursor, to money laundering or terrorist financing, also known as a predicate offence (e.g., arms trafficking, mafia, smuggling, fraud, tax and financial crimes, corruption, cybercrime, bribery) or related security measures;
- You are involved in other AML/CFT related negative or bad news found on reliable and public media sources;
- You have been disqualified or are prohibited from holding positions of responsibility (such as company directorships);
- Your business is related to the production, dissemination or use of virtual currencies;
- Your business is linked to online gaming websites that cannot operate since they lack the authorization of their relevant authority.

SGR Database may contain the following types of information about you:

- Information that helps to identify you (e.g. your name; alias; age/date/year of birth[3]; gender; country of residence; passport details; citizenship; resume/curriculum vitae; photo).
- Personal identification numbers (e.g. social security numbers, national insurance numbers and fiscal code) that are public domain data.
- Family circumstances information (e.g. your marital status and dependents), for example, if you are a PEP or a close associate of a PEP.
- Employment/role and education details: for example, the organisation you work for, public roles (including political, diplomatic, religious, judicial, military and trade union roles), your job title and your education history.
- Professional and personal affiliations: for example, organisations and individuals that you may be associated with in your professional or personal capacity.
- Your inclusion on sanctions or warnings list or watchlist, or on public lists regarding disqualified professional.
- public domain data about actual or alleged money laundering or terrorist financing crime, or crimes that are a pre-cursor to money laundering or terrorist financing which are also known as predicate offences (e.g. financial crime, illegal trafficking, drug, corruption, bribery, environmental offences, smuggling, membership of an organised crime group).
- If you are qualified as a PEP or as a local politician at regional, provincial, municipal and metropolitan city level.

[3] The date can refer to a calculated year. The calculation can only approximate to the exact year of birth (+/-1 year) as it is based on the age of the subject at the time of collection.

- If your business is related to the production, dissemination or use of virtual currencies or to online gaming websites that cannot operate since they lack the authorization of their authorities.
- Your postings on website or social media.

In some cases, the personal information on SGR Database includes so-called “sensitive” or “special categories” of personal information such as:

- information relating to your political status (for example, if you are a PEP holding a position in a political party);
- information relating to your sexual orientation (for example, if SGR records that you are the spouse or partner of a PEP);
- information relating to your religious beliefs (for example, if you are a senior religious leader that qualifies you as a PEP);
- information on your company/entity membership (for example, if this position qualifies you as a PEP);
- information relating to any criminal offences actually or allegedly committed by you (for example, if these are money-laundering or terrorist financing offences, or pre-cursor crimes to such offences), also your inclusion on sanction or disqualified Database.

Categories of recipients to whom the personal data will be disclosed

SGR does not distribute personal data on its Database to the general public.
Databases and the information managed by SGR are saved in our servers located in Switzerland. Access to the servers is only allowed to specific IP addresses (server administrators) that access them through personal and confidential credentials, which are changed periodically.
We make SGR Database information available to a limited number of subjects:

- We only make our information available to Customers that have a legitimate interest to access information. Only authorised Customers have access to the Database. We also require that they only use it for the purposes of carrying out Checks or to otherwise comply with laws. SGR informs Customers about appropriate use of the Database including usage restrictions in its contracts.
- We share information about you to members, consultants and employees of SGR with robust procedures and contractual obligations designed to protect your information.
- We allow a limited number of verified and reputable third parties who provide advice and services to us, and business partners that cooperate with us to make SGR Database available for the purpose of Checks to final common Customers/clients, to access information. For example, service providers who help us maintaining SGR Database (e.g. IT systems providers, hosting providers, providers of technical support).
- We disclose information about you to competent authorities in connection with one or more of the purposes outlined above where we are required to do so or at their request.

How we secure your personal information

We use physical, IT, electronic and managerial measures to keep your personal information secure, accurate and relevant.
These policies and measures include:

- internal policies and procedures, robust controls around the inclusion and maintenance of SGR information which are designed to ensure that information about you on SGR Database is accurate and relevant;
- staff training to ensure that they are aware of and comply with our policies, procedures and controls designed to keep SGR information secure, accurate and relevant;
- administrative and technical controls to restrict staff access to SGR information;
- a business continuity and disaster recovery strategy that applies to SGR and which is designed to safeguard the continuity of access to, and security of, SGR;

- physical security measures, such as strict controls on access to locations of SGR servers;
- monitoring compliance with our policies, procedures and controls.

We also impose contractual restrictions on Customers, counterparts and business partners requiring them to exclusively use information on SGR Database only in connection with Checks or to pursue their contractual duties with us or with final common Customers.

Why information may be transferred abroad

The processing takes place at SGR headquarters. The data are physically stored on the servers located in Switzerland. When we transfer personal information internationally, we put in place safeguards in accordance with applicable laws (DSG and GDPR including Articles 44 to 50), to ensure that when your personal information is transferred internationally, it is subject to appropriate safeguards. These include contractual safeguards.

Criteria used to determine period for which we keep your information

How long your data is held in SGR Database will depend on type of information we hold about you, AML/CFT/KYC requirements and related jurisprudence and doctrine.
As a general not exhaustive information, we base on the following criteria to calculate retention periods for your personal information:

- the length of time your personal information remains relevant to Checks, available to public domain and relevant in the public interest or legitimate interest;
- the length of time it is reasonable to keep records to demonstrate that we have fulfilled our duties and obligations;
- the existence of any relevant proceedings;
- the existence of other relevant history, factors or risk indicators that indicate that you should be monitored (for instance, if you are a PEP or notorious person or involved in crimes or sanctions);
- any retention periods prescribed by AML/CFT/KYC international and national laws or recommended by regulators, professional bodies or associations or inter-governmental bodies.

Your privacy rights

We will honour the privacy rights you have under DSG, GDPR and DPA applicable to SGR, i.e.:

- right to be informed, as set out in Article 19 of the DSG and in Article 14 of the GDPR;
- right of access, as set out in Article 25 of the DSG and Article 15 of the GDPR;
- right to rectification, as set out in Article 32 of the DSG and Article 16 of the GDPR;
- right to erasure or right to be forgotten, as set out in Article 32 of the DSG and Article 17 of the GDPR.

Restrictions on Data Subject's rights are provided for by Articles 30.3, 31 and 32 of the DSG and by Article 15 and 26 of the DPA, especially in connection with a public interest or "*in connection with the safeguarding of national security and with defence*".
Please note that any right you may have to request information, updates or deletions to your personal data on SGR Database is not absolute and we may be lawfully permitted to refrain from making any disclosure, update or deletion to your personal data on SGR Database: should this be the case, we will explain to you why.

If you decide to exercise any of your rights, we will ask for information to verify your identity. This is also done to keep your privacy safe. Any identification evidence that you provide will only be used to verify your identity with the intent to answer your requests. In case you decide to proceed with a request to update or remove your personal data from SGR Database, we will need a written explanation of your request to assess it against applicable laws. Depending on the nature of the request and the personal data involved, we may also ask you to provide supporting information and/or documentation. There are limits to the rights that you have in relation to your personal data and

in certain circumstances we may not be required or able to meet your request, or we may meet your request partially. Where this occurs, we will provide you with an explanation of the legitimate basis on which we are unable or not required to meet your request. Once a decision has been made on a request to update or remove personal data on SGR Database, that decision will be communicated to you.

We operate many controls to prevent incorrect or inaccurate data from being processed on SGR Database. It is critical for us to ensure the accuracy and relevance of personal data on SGR Database. SGR simply collects public information from publicly available sources. However, because of the nature of public domain data, we cannot discount that data we process may contain some errors or become outdated. Therefore, if you find an error in any personal data that we process, fill out the form at the following link: https://www.sgrdailycontrol.com/dcrights.cfm.

How to contact us

If you wish to submit a request to exercise any of your rights thinking that you are present in SGR Database, please fill out the form at the following link: https://www.sgrdailycontrol.com/dcrights.cfm.

Changes to this privacy policy

We may modify or amend this Privacy Policy from time to time.
Any future changes or additions to the processing of personal information as described in this Privacy Policy affecting you will be communicated to you through updating of this Privacy Policy.

Supervisory Authority

EDÖB is responsible to advise, educate and ensure the protection of personal data in Switzerland.
Office of the EDÖB is at
Feldeggweg 1 CH - 3003 Berne
Telephone: +41 (0)58 462 43 95 (mon. - fri. 10-12 am)
Telefax: +41 (0)58 465 99 96

Or pursuant to DPA, the UK Information Commissioner's Office ("**ICO**")
Wycliffe House, Wilmslow, Cheshire, UK.

(Updated JUNE 2021)