



## General Terms and Conditions

### 1. General

These general terms and conditions ('T&Cs'), and any other documents to which the T&Cs refer (together 'Contract'), regulate the contractual relationship between you as a User ('User') and Qnister AB, reg. no. 559116-6433, ('Qnister', 'we' or 'us') (individually 'Party' and jointly 'Parties') concerning the User's use of Qnister's cloud service Qnister Screening as further described under Section 2 below, ( the 'Service').

By starting to use the Service, the User confirms that it has read and understood and is bound by the rights and obligations under the Contract.

### 2. The Service

Qnister will according to applicable price list from time to time make available to the User the possibility to perform searches in its cloud based service Qnister Screening. The User will share data with and get access to data from Qnister's licensor Open Sanctions, Softwareentwickler (VAT-ID DE344342340) (the "Licensor"). The data will include data from OpenSanctions Consolidated Sanctions data (including UN Security Council Consolidated Sanctions, the EU Financial Sanctions Files, the UK Treasury Consolidated sanctions list and the Swiss SECO sanctions list).

The User is obligated to follow the instructions that are provided concerning the use of the Service and at all times follow and comply with the Contract.

### 3. Permitted Use

The User may only use all or part of the Data for personal or commercial purposes with the aim to adhere to applicable sanction regulations. The User shall not, directly or indirectly, use the Data or any part thereof to conduct or operate any bulk mail activity, whether conducted electronically or via any governmental or commercial carrier.

Except as otherwise expressly provided in this Contract, the User shall not, in whole or in part: (i) resell, rent, lease or loan the Data in whole or significant part to third parties; (iii) disseminate the Data, whether in print, online, by email or by other means to third parties; (iv) disclose the Data to any third party.

Except as expressly set forth herein, all other rights and title in and to the Data are reserved to Qnister and the Licensor.



#### 4. **No warranty and Limitation of liability**

Qnister through its Licensor will make a reasonable and timely effort to ensure the accuracy of the Data delivered to the User. HOWEVER, QNISTER AND ITS LICENSOR OFFERS NO WARRANTY AS TO THE COMPLETENESS, ACCURACY OR ENTIRELY OF THE DATA AND ASSUMES NO LIABILITY FOR MISTAKES, INACCURACIES OR INCONSISTENCIES CONTAINED THEREIN. ACCORDINGLY, THE USER ASSUMES ALL LIABILITIES AND RESPONSIBILITIES FOR ANY ACTIONS TAKEN OR NOT TAKEN REGARDING USER'S USE OR NON-USE OF DATA. In the event the User identifies such a mistake, inaccuracy or inconsistency in the Data, the User shall use reasonable efforts to notify Qnister of such mistake, inaccuracy or inconsistency in a timely manner.

#### 5. **Intellectual property rights**

The Service and its content, including but not limited to texts, documents, images, layouts, logos, source code (jointly 'Content') and any associated rights (such as copyright, trademark protection or patent, regardless of whether they are registered) are held by or licensed to Qnister or its partners and suppliers. The Contract do not entail the transfer of any of these rights to the User.

It is not permitted to fully or partially copy, modify, reproduce, reuse, make available, share, transmit, adapt, translate, use to create adapted works, sell, transfer, sub-license, or otherwise exercise control or take any actions beyond normal use as regards the Service.

The User does not have the right to decompile or disassemble the Service without Qnister's explicit permission, other than where explicitly stipulated by law.

#### 6. **Personal data processing**

When the User performs searches in Qnister Screening, the search data is transferred to the Licensor. Qnister performs this transfer as a processor on behalf of the User according to what is set out in Data Processing Agreement, Appendix 1.

#### 7. **Conflict of law and dispute resolution**

Disputes arising from the Contract shall ultimately be resolved through arbitration in accordance with the Expedited Arbitration Procedure of the Arbitration Institute of the Stockholm Chamber of Commerce. Arbitration shall take place in Jönköping and proceedings shall be held in Swedish.



The Contract shall be governed by Swedish law excluding its choice of law principles.

## APPENDIX 1

# Data Processing Agreement

## Parties

This data processing agreement ('DPA') regulates the terms and conditions between you as a User ('Controller') and Qnister AB ('Processor'), individually designated 'Party' and jointly 'Parties', concerning the Processor's Processing of Personal Data on behalf of the Controller.

### 1. Background and Definitions

- 1.1. The Controller wants to use the Service Qnister Screening in accordance with the T&C's.
- 1.2. The Processor facilitates the search which means that the search data that is inserted in the Service is processed on the Processor's servers. The Processor further transfers the search data to the Licensor, that constitutes a third party controller and re-transfers if there is a hit or not on one of the available sanction lists.
- 1.3. Unless otherwise stated, terms shall have the same meaning as in the General Data Protection Regulation.

### 2. Responsibilities of the Controller

- 2.1. The Controller is responsible for the Processing of Personal Data being legal and taking place in accordance with the applicable Data Protection Regulations.
- 2.2. The Controller shall only provide the Processor with access to the personal data that is necessary with consideration for the purpose of the Processing.
- 2.3. The Controller shall immediately provide the Processor with correct information in the event of the instructions being incorrect, incomplete or otherwise in need of amendment.

### 3. Personal Data Processing

- 3.1. The Processor shall only process Personal Data in accordance with this DPA, Applicable Data Protection Regulations and the Controller's instructions applicable at any time; see



Sub-appendix 1.

- 3.2. The Processor may not process Personal Data for their own or any other purposes than those for which the Processor has been engaged by the Controller.
- 3.3. The Processor may not transfer Personal Data to a Third Country unless this is permitted in accordance with the contents of Appendix 1.
- 3.4. The Processor shall without unreasonable delay, and at most within thirty (30) days of the Controller's request, provide the Controller with access to the Personal Data that the Processor possesses and implement a requested alteration, erasure, restriction or transfer of Personal Data. If the Controller has erased, or instructed the Processor to erase, the latter shall take such measures as necessary to prevent restoration of the Personal Data.
- 3.5. The Processor is obligated to maintain a record of the Processing that takes place on behalf of the Controller. Upon request, a copy of this record shall be provided to the Controller or the competent supervisory authority in a readable format.

## **4. Security measures and audits**

- 4.1. The Processor shall via appropriate technical and organisational measures restrict access to the Personal Data and only provide authorisation to personnel who require access to the Personal Data in order to fulfil their commitments under this DPA, as well as ensure that such personnel have the necessary training and have received sufficient instruction in how to handle the Personal Data in an appropriate and secure manner.
- 4.2. The Processor shall without unreasonable delay, notify the Controller about the occurrence or risk of a Personal Data Breach. Such notification shall include all necessary and available information that the Controller requires in order to take appropriate preventative measures and countermeasures, as well as to fulfil its obligations as regards notifying the competent supervisory authority of Personal Data Breaches.
- 4.3. The Processor shall at the request of the Controller, or an independent third party engaged by the Controller, enable and contribute to audits and/or providing other adequate proof of compliance. The Processor shall ensure that the Controller has the equivalent rights in relation to any engaged Sub-Processors.



## **5. Cooperation**

- 5.1. The Processor shall, to the extent provided by law, assist the Controller in ensuring that the obligations concerning rights of data subjects, Personal Data Breaches and impact assessments.
- 5.2. The Processor shall without unreasonable delay inform the Controller if the Processor has been contacted by the competent supervisory authority or another third party in order to gain access to the Personal Data that the Processor, or in applicable cases Sub-Processor, has in its possession.

## **6. Sub-Processor**

- 6.1. The Processor has engaged sub-processors according to what is set out in sub-appendix 1.
- 6.2. It is the responsibility of the Processor to ensure that a Sub-Processor fulfils all applicable stipulations on the protection of Personal Data and fulfils the obligations regulated by this DPA.

## **7. Transfer to a Third country**

- 7.1. The Processor may not transfer data to a Third country without prior written approval from the Controller.



Sub-appendix 1

## **Instructions for processing of personal data**

### **Purpose of the processing**

The Processor facilitates the search in a third party's (the Licensor's) consolidated sanctions list which means that the search data that is inserted in the Service is processed on the Processor's servers. The Processor further transfers the search data to the Licensor, that constitutes a third party controller and re-transfers if there is a hit or not on one of the available sanction lists.

### **Type of processing**

Search data is matched with Licensor's Consolidated sanction list.

### **Type of personal data**

- Name
- Company registration number (could constitute personal data in some cases)

### **Special categories of personal data**

The use of the Service does not require processing of special categories of personal data.

### **Geographic location of the processing**

The personal data is processed on a server located within the EU/EEA.

### **Duration of the processing**

The Controller does not store any search data after the search process has been finalised.



## Sub-processor

Name	Description	Geographic location
GleSYS AB	Data servers	Sweden
Microsoft Azure	Personal data processing for administration of user accounts.	EU/EES. Even if personal data is stored within EU/EES the personal data might, according to American laws, be transferred to the United States as Microsoft parent company is an US entity.