Last updated: [March 11th, 2020]

Privacy Notice – Blockchain.ey.com Authentication Service

1. Introduction

This Privacy Notice is intended to describe the practices EY follows in relation to the Blockchain.ey.com ("BEC") Authentication Service ("AS") (the "Tool") with respect to the privacy of all individuals whose personal data is processed and stored in the Tool.

2. Who manages the Tool?

"EY" refers to one or more of the member firms of Ernst & Young Global Limited ("EYG"), each of which is a separate legal entity and can act as a data controller in its own right. The entity that is acting as data controller by providing this Tool on which your personal data will be processed and stored is EYGM Limited an EY global entity.

The personal data in the Tool is shared by EYGM Limited with one or more member firms of EYG (see "Who can access your personal data" section below).

The Tool is hosted on servers externally in an EY Managed MS Azure Data Centre in Eastern USA.

3. Why do we need your personal data?

The Tool focuses on user login authentication. AS provides registration, login and authentication for the BEC platform. It returns an authentication token that can be used to authenticate API requests to platform services.

Your personal data processed in the Tool is used as follows: Data is used to authenticate the individual or company. The EY independence team will review the data provided to determine whether the individual/ company is "Channel 1" or "Channel 2". This determination will impact the level of information and services that they will be able to use on BEC.

EY relies on the following basis to legitimize the processing of your personal data in the Tool:

Processing of your personal data is necessary for the purposes of the legitimate interests pursued by the data controller 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. The specific legitimate interest is Quality & Risk Management, including complying with EY policies.

4. What type of personal data is processed in the Tool?

The Tool processes these personal data categories:

- Full Name;
- Email Address;
- Country where the individual is located;
- Company name and jurisdiction of incorporation; and

- Password.

This data is sourced from:

- EY Partners, employees or contractors; and
- A feed from other EY systems, being EY's Global Human Resources Database.

Sensitive personal data

Sensitive personal data reveals your racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning sex life or sexual orientation.

EY does not intentionally collect any sensitive personal data from you via the Tool. The Tool's intention is not to process such information.

5. **Who can access your personal data?**

Your personal data is accessed in the Tool by the following persons/teams:

EY	Client
• EY Users • EY Independence team	• Client Users

Role	Location	Access purpose	Access rights
EY Users	Global	To authenticate user details.	Read, write and delete rights.
EY Independence team	United States	To verify if users are affiliated with SEC audit clients and whether they are channel 1 or channel 2 users.	Read only.
Client Users	Global	To authenticate user details.	Read, write and delete rights.

The access rights detailed above involves transferring personal data in various jurisdictions (including jurisdictions outside the European Union) in which EY operates (EY office locations are listed at www.ey.com/ourlocations). An overview of EY network entities providing services to external clients is accessible here (See Section 1 (About EY) - "View a list of EY member firms and affiliates"). EY will process your personal data in the Tool in accordance with applicable law and professional regulations in your jurisdiction. Transfers of personal data within the EY network are governed by EY's Binding Corporate Rules.

We transfer or disclose the personal data we collect to third-party service providers (and their subsidiaries and affiliates) who are engaged by us to support our internal ancillary processes. For

example, we engage service providers to provide, run and support our IT infrastructure (such as identity management, hosting, data analysis, back-up, security and cloud storage services) and for the storage and secure disposal of our hard copy files. It is our policy to only use third-party service providers that are bound to maintain appropriate levels of data protection, security and confidentiality, and that comply with any applicable legal requirements for transferring personal data outside the jurisdiction in which it was originally collected.

For data collected in the European Economic Area (EEA) or which relates to individuals in the EEA, EY requires an appropriate transfer mechanism as necessary to comply with applicable law. The transfer of personal data from the Tool to EY users, the EY independence team and client users is governed by an agreement between EY and the service provider that includes standard data protection clauses adopted by the European Commission.

6. Data retention

Our policy is to retain personal data only for as long as it is needed for the purposes described in the section "Why do we need your personal data". Retention periods vary in different jurisdictions and are set in accordance with local regulatory and professional retention requirements.

In order to meet our professional and legal requirements, to establish, exercise or defend our legal rights and for archiving and historical purposes, we need to retain information for significant periods of time.

The policies and/or procedures for the retention of personal data in the Tool are in accordance with EY Records Retention Global Policy and the applicable Global, Area, Region or Country Retention Schedule.

Personal data is stored for the duration you maintain, and actively use, your profile on the Tool. After a period of inactivity of 7 years, your personal data will be deleted.

After the end of the data retention period, your personal data will be deleted.

7. Security

EY protects the confidentiality and security of information it obtains in the course of its business. Access to such information is limited, and policies and procedures are in place that are designed to safeguard the information from loss, misuse and improper disclosure. Additional information regarding our approach to data protection and information security is available in our Protecting your data brochure.

8. Controlling your personal data

EY will not transfer your personal data to third parties (other than any external parties referred to in section 6 above) unless we have your permission or are required by law to do so.

You are legally entitled to request details of EY's personal data about you.

To confirm whether your personal data is processed in the Tool or to access your personal data in the Tool or (where applicable) to withdraw your consent, contact your usual EY representative or email your request to global.data.protection@ey.com.

9. Rectification, erasure, restriction of processing or data portability

You can confirm your personal data is accurate and current. You can request rectification, erasure, restriction of processing or a readily portable copy of your personal data by contacting your usual EY representative or by sending an e-mail to global.data.protection@ey.com.

10. Complaints

If you are concerned about an alleged breach of privacy law or any other regulation, contact EY's Global Privacy Leader, Office of the General Counsel, 6 More London Place, London, SE1 2DA, United Kingdom or via email at global.data.protection@ey.com or via your usual EY representative. An EY Privacy Leader will investigate your complaint and provide information about how it will be handled and resolved.

If you are not satisfied with how EY resolved your complaint, you have the right to complain to your country's data protection authority. You can also refer the matter to a court of competent jurisdiction.

Certain EY member firms in countries outside the European Union (EU) have appointed a representative in the EU to act on their behalf if, and when, they undertake data processing activities to which the EU General Data Protection Regulation (GDPR) applies. Further information and the contact details of these representatives are available here.

11. Contact us

If you have additional questions or concerns, contact your usual EY representative or email global.data.protection@ey.com.