Privacy Statement – Emergency Response Application (ERA)

1. Introduction

This Privacy Statement is intended to describe the practices EY follows with respect to the privacy of all individuals whose personal data is processed and stored in the EY ERA application. This Privacy Statement should be read together with the ey.com Privacy Statement, and in case of any conflict with the ey.com Privacy Statement, the terms of this Privacy Statement will prevail. Please read this Privacy Statement carefully.

2. Who manages the application?

"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 determine the purposes and means for data processing in its own right (i.e. act as a data controller or in a similar capacity). The entity that is acting as data controller (or similar capacity) by providing this application on which your personal data will be processed and stored is EY Global Services Limited and it licenses the cloud platform from SAP, Hasso-Plattner-Ring 7, 69190 Walldorf, Germany.

The personal data in the application is shared by EY Global Services Limited with one or more member firms of EYG (see "Who can access your personal data" section 6 below).

The application is hosted by EY on SAP datacentres.

3. Why do we need your personal data?

The EY ERA application enables the user(s) to search for products- as provided by the NGOs and provide them with the address(es) of the distribution centres, where they can find these products.

Your personal data processed in the application is used as follows:

For users – Upon approval from the user, the application will collect their geo location to help search for the distribution centres closest to them. No other data is collected.

For NGOs – Your data - NIP and REGON numbers, NGO name, phone number, head office location, email, emergency contact person provided during the login process and distribution centres locations is used to help users find the products they need.

EY also uses the above-mentioned data to create dashboards; allowing NGOs to source the products in demand by the users based on their location.

Your personal data such as email address/NIP/REGION/Phone number will be encrypted and only be used to permit proper user authentication in the application while providing you with the ability to delete your account as and when needed.

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

The application processes these personal data categories:

For users (People searching for products on the application) – Only the user's location (after giving permission) will be collected. No other data will be collected or processed.

For NGOs registered on the application – EY collects the data of the products available in different distribution centres. Along with NIP and REGON numbers, NGO name, contact name and number, head office location and email.

5. 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 ERA does not collect any sensitive personal data.

6. Who can access your personal data?

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

USER GROUP	LOCATION	PURPOSE	ACCESS LEVEL	Count
EY (Service Administrators and Onboarding team)	Globally	Creating accounts for new EY ERA NGOs and provide access to all features.	Full access to all data (including personal data)	3
EY (Engineering team)	Globally	Specific debugging issues.	Full access to all data (including personal data)	3
EY (Engineering team)	Globally	Analytics.	Full access to all data (including personal data)	3
EY (Engineering team)	Globally	Maintenance and Support	Full access to all data (including personal data)	3

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 https://www.ey.com/en_gl/locations). 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 application 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 application to SAP, are governed by agreements between EY and the service providers that includes standard data protection clauses adopted by the European Commission.

7. How your data will be processed by Adobe Analytics

The Emergency Response Application (ERA) also use Adobe Analytics ("Adobe") in order to provide reporting, visualisations and analysis of data. Your personal data will be processed by Adobe for the following purposes: (i) to capture web metrics about the journey of users within our websites and applications (e.g. pages viewed and links clicked); (ii) to analyse and understand overall site traffic information; (iii) to allow us to make informed decisions about our intranet and extranet web sites; and (iv) to authenticate users and permit them to access Emergency Response Application (ERA). EY Global Services Limited is the data controller for the purposes of this processing and licenses Adobe from Adobe Systems Software Ireland Limited, 4-6 Riverwalk, Citywest Business Campus, Saggart, Dublin 24, Ireland, who hosts it in London, United Kingdom. Adobe processes the following types of personal data in relation to its users: [username (relating to system administrators only); hashed email address; user rank; user business unit; user service line; user sub service line; user sub management unit (SMU); user sector; user area; user sub area; user country; user country code; user region/office; FSO, Financial Service Office; GDS, Global Delivery Service; and/or internal vs. external user information. This personal data will be retained for 37 months and archived for 90 days before deletion. Sensitive personal data relating to 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, is not processed. This personal data can be accessed by Emergency Response Application (ERA) Team. This processing is necessary for the purposes of the legitimate interests pursued by us (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 pursued is: reporting on the usage of our applications and website.

8. 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 application are:

- The total retention period is defined and will be implemented in accordance with the EY Records Retention Global Policy and the relevant Country Retention Schedule (CRS).
- NGO's account will be terminated from the application after it's been inactive for 6 months. Alternatively, data may also be deleted by the NGO at any time using the standard web interface.
- For users, geo location data is monitored only during the active session and is not saved in our database.
- Upon termination of your account in the application, aggregated and anonymised results are retained for 30 days. After this period, the backup data of such data will be kept for 90 days preceding which the data won't be recoverable.
- Log Data will be retained in accordance with the EY IT Logging Policy. After the end of the data retention period, your personal data will be deleted.

9. 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.

10. 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 application or to access your personal data in the application or (where applicable) to withdraw your consent, email your request to global.data.protection@ey.com or for Polish users to kontaktdaneosoboweEYPolska@pl.ey.com.

11. Object, rectification, erasure, restriction of processing or data portability

You can confirm your personal data is accurate and current. You can object to the processing of your personal data or 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 or for Polish users to kontaktdaneosoboweEYPolska@pl.ey.com.

12. 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 for Polish users at kontaktdaneosoboweEYPolska@pl.ey.com. 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.

13. Contact us

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

14. Acknowledgement

Upon your electronic acknowledgement, the terms contained in this Privacy Statement are deemed effective as of the date of that acknowledgement and shall remain effective until your account is active on the EY ERA application.