Privacy Statement[1] – Ready for Crisis (R4C)

1. Introduction

The Single Resolution Board (SRB) processes your personal data in accordance with the Regulation (EU) 2018/1725 (EUDPR). The privacy statement explains the reasons for processing your personal data, the way the SRB collects, handles and ensures protection of all personal data. It also specifies the contact details of the responsible SRB unit where you may exercise your rights, the SRB Data Protection Officer and the European Data Protection Supervisor (EDPS)

2. Who is responsible for processing your personal data?

The SRB is the controller for processing the personal data. The specific SRB unit responsible for the processing of your personal data is Unit 03 Crisis Preparedness and Management.

3. Why do we process your personal data?

R4C is the IT application for Crisis Management at SRB. It intends to improve:

- The quality and availability of information to support crisis management processes.
- The collaboration and real-time exchanges of information between a high number of stakeholders via a single platform.
- Overall efficiency in the execution of all the tasks required in crisis management (document management, planning, monitoring and control of the crisis process).

The purpose of the processing of the personal data is the following:

- Support Crisis Management Teams in crisis management processes.
- Creation of an access account to the system.
- Monitoring reports and consolidated reports for senior management.
- Sending communications, such as assigned tasks, via email to the Crisis Management Team members

4. What are the legal bases for processing your personal data?

The processing of personal data is necessary for the performance of tasks carried out in the public interest by the SRB -which is the management and functioning of the SRB- and for compliance with the SRB's legal obligations pursuant to Article 5(1) (a) and (b) of the EUDPR in conjunction with Articles 58, 59 and 65 of the SRMR.

5. What categories of personal data are processed?

[1] Last update on 27/02/2023

The categories of data processed are the following:

Data in R4C: Team information handling a crisis (First Name, Last Name, Unit, Phone number, Function and Company). This information is shared between the team members involved in the crisis cases on a strictly need-to-know basis. For all other users, this is very strictly shielded.

Data for access management: R4C collects personal data exclusively to the extent necessary to fulfil the access management. The information will not be re-used for any other or any incompatible purpose. Access to R4C requires the existence of an IAM (Identity and Access Management) account, the latter being managed by the SRB in a dedicated system, based on the following credentials: First Name, Last Name, E-mail and Unit. For external contributors, in addition Phone Number, Contact Type and Company is collected. A user-id and password are given back to logon in R4C.

Data for reporting shared with senior management: Most attributes of the R4C application might be used to generate consolidated reports and provided to senior management of SRB or NRA's, when relevant. Personal data such as the First and Last name may be used to produce an audit trail for all crisis cases of the application.

6. Who has access to your personal data?

When the SRB processes personal data for the aforementioned purposes, the following persons may access your personal data on a strict need-to-know basis:

- The staff members of Unit 03 Crisis Preparedness and Management;
- The SRB ICT staff;
- Other staff employed by the SRB and participating in a crisis case;
- National Resolution Authorities and the institutions under their jurisdiction that are in scope of Article 2 SRMR; and
- External Counsel of the SRB and its sub-contractors (external advisor firm, external consulting firm) who process personal data on behalf of the SRB and under the instructions of the SRB.

R4C will only disclose data to third parties if that is necessary for the fulfilment of the purpose(s) identified above and to the mentioned (categories of) recipients. The SRB will not divulge your personal data for direct-marketing purposes.

7. In which third country personal data could be transferred?

Personal data is not transferred to third countries. The data remains on the SRB's infrastructure.

8. How long will the SRB keep your personal data?

The SRB only keeps the data for the time necessary to fulfil the purpose of crisis management while respecting the retention guidelines applicable under the Records Management Policy at the SRB.

9. What are your data protection rights?

You have the right to access your personal data and correct any data that is inaccurate or incomplete. You have also (with some limitations) the rights to delete your personal data, to restrict tor to object to he processing of your personal data in line with the Regulation (EU) 2018/1725.

10. Who can you contact in case of queries or requests?

You can exercise your rights by contacting the SRB's Unit 03 Crisis Preparedness and Management at SRB-RTT@srb.europa.eu. The SRB's Data Protection Officer at SRB-DPO@srb.europa.eu, answers all queries relating to your rights under the EUDPR.

11. Addressing the European Data Protection Supervisor

If you consider that your rights under Regulation (EU) 2018/1725 have been violated as a result of the processing of your personal data, you have the right to lodge a complaint with the European Data Protection Supervisor at any time.