In Case of Crisis
by RockDove Solutions

# RDS COMPLIANCE WITH GDPR

2018

*The following document outlines the status of the RockDove Solutions, Inc. platform, In Case of Crisis with regards to the specific requirements regarding the transfer of data out of the EU. As the US is not specifically listed as one of the countries that meets the GDPR requirements, RockDove Solutions is also undertaking the steps necessary for Privacy Shield certification to show adequate protection allowing for the transfer of personal data from the EU to US.*

## REQUIREMENTS AND PRINCIPLES CONFIRMED

In Case of Crisis has always maintained the absolute minimum amount of personal information necessary for the operation of its services. As such, no private information is stored or requested from individuals or organizations unless that information is necessary for the In Case of Crisis operations and to provide the appropriate safety information to the approved personnel when necessary at the time of a crisis situation.

As security has been paramount to providing a safe solution, the In Case of Crisis platform has followed the highest level of security and encryption standards for both their online portal and the mobile application.

With ongoing third-party security vulnerability and penetration testing by Trustwave along with Spyderlabs, In Case of Crisis has validated their security solution and has constantly evolved to mitigate the ever growing list of new threats and vulnerabilities.

### Specific Privacy Areas Confirmed

- A Privacy Policy has been documented and is reviewed annually for compliance with applicable privacy and data protection laws and regulations.
- Procedures, Roles and Permissions have been developed to maintain the security, confidentiality, and protection of customer information.
- A documented system architecture is maintained showing where data is stored and how security and encryption are implemented.
- A Data Privacy Officer has been delegated for RockDove Solutions, Inc. to work alongside the Security Officer and Senior System Administrator to ensure workflows and procedures are in keeping with stated policies and regulations.
- Clients are provided access to view, update, and purge all user and privacy information related to their organization.
- All data is hosted within the continental US using certified cloud hosting providers, Amazon AWS and Microsoft Azure. Full encryption is accomplished using the Azure Transparent Data Encryption (TDE) algorithms for both the primary and real-time replicated secondary storage. Mobile app encryption is accomplished using cypher and crypto libraries and those have been registered with the Department of Commerce, Bureau of Industry and Security, SNAP-R, Supplement No 5 to Part 742 – Encryption Classification.
- A Privacy Policy is published and made publicly available and reviewable at all points where personal information is received from an individual.
- All personal information is obtained for specified and lawful purposes and is not further processed or disclosed in any manner incompatible with these purposes.

- Processes are in place for users to challenge, update and/or correct their personal information.
- Controls are in place to validate the personal information obtained from individuals before using their information.
- Hidden fields with individuals' personal information are not in use within the application.
- Personal information is not stored within cookies or cached within pages of the application and is only stored within the encrypted data stores for use by the application when in use. Access to personal information by the application is validated annually to be fully secure by third-party penetration testing.
- Ongoing Privacy training annual security certification is performed for all RockDove Solutions, Inc. staff.
- Privacy Impact Assessments are performed for each new functionality during the requirements phase when developing or purchasing new systems or services as part of the development lifecycle.

## REQUIREMENTS AND PRINCIPLES ADDRESSED IN RELEASE 4.3

In order to meet the full requirements of the GDPR laws as both controller and under contract as a processor for our clients, the following workflows and procedures were incorporated into the In Case of Crisis solution, including enhancements to both the Mobile application and Online Administration portal.

- Workflows were added to prompt end-users and record consent and versioning of data privacy policies prior to allowing entry of privacy information.
- Functionality was added for end-users to review their information and upon request, have their individual attributes removed from the In Case of Crisis system within a 30-day timeframe while working with the individual's clients (the Controllers) from whom this information was received in the use of an ongoing and active organizational plan.
- Retention and categories of information was audited for completeness with the latest functionality of In Case of Crisis and functionality was added to ensure the pseudonymisation of user account information when requested.
- Data portability and extract measures were developed to respond to data subject's requests to provide all personal information either directly to data subject or in a format that enables the transfer of their information to a controller.
- Updated our policies and procedures to ensure that in the event of a data breach and solid evidence of data exposure, data subjects and/or their relevant organizations are notified within 72 hours.

## PRIVACY SHIELD CERTIFICATION

As the US is not specifically listed as one of the countries that meets the GDPR requirements, RockDove Solutions is undertaking the steps necessary for Privacy Shield certification to show adequate protection allowing for the transfer of personal data from the EU to US.

## REGULATION COMPLIANCE STATUS

RockDove Solutions exercises reasonable efforts to correct any Error reported by clients and by our automated alert notifications systems in accordance with the priority level reasonably assigned to such Error by our Cloud Providers.

Should you desire to see all the data RockDove Solutions maintains on your behalf, please contact privacy@rockdovesolutions.com.