Data Breach and Incident Management Policy

«RC GmbH» adopts the following Data Breach and Incident Management Policy as an integral part of its corporate strategy and in compliance with the General Data Protection Regulation ("GDPR").

This document provides information about:

(a) «RC GmbH» as the controller,
(b) the purpose and scope of the policy,
(c) the structure of the data breach notification system, and
(d) the relationship with existing policies of the controller.

A. Name and contact details of the controller

«RC GmbH»

«Fraunhoferring »«3»

«85737»«Ismaning»

Phone: «089-72637910»

Email: «info@remarketing.company»

B. Purpose and scope of the policy

«RC GmbH» in its capacity as the controller in the scheme of GDPR wishes to establish a data breach and incident management policy to ensure the security of all personal data during its lifecycle, including clear lines of responsibility. This policy sets out the procedure to be followed to ensure a consistent and effective approach is in place for managing data breach and information security incidents. The purpose of this policy is to set out the framework of the notification system and inform and support all people involved in data processing in all areas of the organization in adhering to this notification system.

The policy applies to all employees, freelancers, independent contractors of «RC GmbH» and any other person who is in general in any way involved in data processing operations and has permanent or temporary access to personal data. It also covers all personal data the controller gathers and processes.

C. Data breach notification system

The concept of “data breach” holds a central position in the data protection legislation. In the framework of GDPR, a personal data breach is understood as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed (Article 4(12) GDPR). This concept is combined with notification obligations of the controller and the processor. To comply with the requirements of the Regulation, the controller has established and presents herein a notification procedure, and it takes reasonable care to inform all people involved to data processing in its organization about the procedure and keep them updated.

1. Identification and obligation to notify for a data breach

All people involved in processing of personal data shall immediately inform the controller and its Data Protection Officer about the possibility of a data breach. For the handling of these incidences, the controller has established internal procedures in order to be able to promptly address the case and assess the risk of the possible breach.

In case of a data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the supervisory authority competent, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. If the notification is not made within this period, it shall be accompanied with reasons for the delay (Article 33(1) GDPR). However, where, and in so far as, it is not possible to provide all information to the authority at the same time, the information may be provided in phases without undue further delay.

Accordingly, every processor shall notify the controller about a potential data breach without undue delay after becoming aware of it (Article 33(2) GDPR). For this reason, the controller pays careful attention to ensure that every processor it engages will conform with his notification obligation.

Secondly, the controller shall also communicate the personal data breach to the data subject without undue delay, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons (Article 34(1) GDPR).

2. Content of the data breach notification

The data breach notification to the supervisory authority shall at least contain the following information:

(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned,
(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained,
(c) describe the likely consequences of the personal data breach, and
(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

When it comes to informing the data subject, the notification shall contain at least the information under (b), (c) and (d) above.

3. Documentation of data breaches

«RC GmbH» documents every personal data breach, comprising the facts relating to the breach, its effects and the remedial action taken with the purpose to enable the supervisory authority to verify compliance with the Regulation (Article 33(5) GDPR) and held the controller accountable, regardless of whether or not a breach shall be notified to the supervisory authority. The retention period of this documentation is determined according to the principles of data protection, if there is personal data contained.

4. Exceptions

The notification of the supervisory authority is not necessary when the breach is unlikely to result in a risk to the rights and freedoms of natural persons (Article 33(1) GDPR). Regarding the notification of the data subject, the controller is not obliged to proceed to notification towards

the data subject if the breach is unlikely to result in a high risk to the rights and freedoms of natural persons, or if any of the following conditions are met:

(a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorized to access it, such as encryption,
(b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialize, and
(c) it would involve disproportionate effort (Article 34(1) and (3) GDPR).

D. Relationship with existing policies of the controller

This Data Breach and Incident Management Policy constitutes an integral part of the controller's data protection management system. For its effective implementation, it shall be applied in combination with the other data protection policies of the controller, even if it results to exemptions. Thus, the controller is responsible to provide guidance as regards their combined implementation and to contribute to the resolution of possible conflicts.

The foregoing Data Breach and Incident Management Policy is set in force by the controller and shall be respected by all related parties involved in the processing of personal data falling into the scope of GDPR. The controller informs about the obligation and ensures that:

(a) all people involved in the processing of personal data understand that they are responsible for following good data protection practice,

(b) All persons involved are aware that a breach of the rules and procedures identified in this policy shall be regarded as a breach of the underlying relationship with the controller,

For additional information and any question regarding the application of this policy, please contact «RC GmbH» or its Data Protection Officer (DPO).

«RC GmbH»
«Ismaning», the «05.11.2020»
«Nils»«Beckmann»
«GESCHÄFTSFÜHRER»