Data Breach Notification Policy

Purpose

AllCode's Data Breach Notification Policy ("Policy") has been developed to provide for a reasonable and consistent response to data breach incidents involving Personal Data. The objective of this Policy is to ensure that AllCode responds appropriately to data breaches and ensures that the appropriate notifications are made when necessary, in compliance with Applicable Laws.

Compliance with this policy is in place to both minimize potential damages that could result from a data breach and to ensure that parties affected by a data breach are properly informed of how to protect themselves.

Definitions

- "Customer" means a third party that has entered into a binding, written agreement with AllCode for the provision of Services.
- "Customer Personal Data" means any Personal Data Processed by AllCode on behalf of a Customer pursuant to or in connection with a customer agreement;
- "Employee" means a natural person employed by AllCode for wages or salary.
- "Employee Personal Data" means any Personal Data of natural persons Processed by AllCode in connection with the performance of a contract of employment or for purposes of recruitment.
- "GDPR" means EU General Data Protection Regulation 2016/679;
- The terms, "Commission", "Controller", "Data Subject", "Member State", "Personal Data", "Personal Data Breach", "Processing" and "Supervisory Authority" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly

Scope

This Policy applies in the event of a Personal Data Breach under Article 33 of the GDPR – Notification of a personal data breach to the supervisory authority – and Article 34 – Communication of a personal data breach to the data subject.

This Policy is applicable to all directors, officers, and employees of AllCode and any other individual or entity acting for or on behalf of AllCode, whether operating inside or outside the United States (collectively "Covered Persons"). Third parties, including but not limited to consultants, agents, intermediaries, and joint-venture partners, must be informed about this Policy and agree to comply with its tenets.

DATA BREACH RESPONSE TEAM

The following positions/individuals will constitute AllCode's Data Breach Response Team (or "Team") for purposes of this Policy:

- Chief Technology Officer
- Head of Product
- Director of Operations / Customer Support Representative

Personal Data Breach

Customer Personal Data

AllCode shall notify Controller without undue delay after becoming aware of a Personal Data Breach. Such notification shall at least: (i) 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; (ii) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained; (iii) describe the likely consequences of the personal data breach; and (iv) 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. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

Employee Personal Data

To the Data Subject

AllCode shall, without undue delay and, where feasible, communicate the personal data breach to the data subject. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).

To the Supervisory Authority

AllCode shall, without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the Personal Data Breach to the supervisory authority in accordance with Article 55. 2 Such notification shall at least: (i) 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; (ii) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained; (iii) describe the likely consequences of the personal data breach; and (iv) 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. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.