

Personal Data Breach Notification Form

Notification Details

|  |  |
| --- | --- |
| **Name**: | John Hamilton |
| **Title:** | Chief Executive Officer |
| **Organization Name**: | Defradar Technologies |
| **Organization Address:** | 3 Hamilton street  Moscow, Russia |
| **Phone number**: | +79 1234 567 8910 |
| **Email Address:** | John.Hamilton@company.com |
| **Date and Time Notification Submitted:** | 27 May 2018 14:00 |
| **Date and Time of Detection of the Data Breach:** | 26 May 2018 10:00 |
| **Elapsed Time Between Detection and Notification:** | 28 hours |

# Description of the Nature of the Personal Data Breach

|  |
| --- |
| An unpatched vulnerability in a module of our website software allowed an unknown party to access confidential customer records and download them to an unauthorised computer via the Internet.  We believe that approximately ten million records have been accessed, consisting of customer names, addresses, tax codes and dates of birth for approximately the same number of data subjects, located in the United Kingdom, Germany and The Netherlands. |

# Likely Consequences of the Data Breach

|  |
| --- |
| This breach may expose the affected data subjects to a high risk of fraud using the contact and personal details stolen. |

# Measures Already Taken to Address the Breach

|  |
| --- |
| The vulnerability that was exploited as part of the attack has now been patched. A complete vulnerability scan has been conducted of our website by a competent third party. We have conducted a full risk assessment and have put in place additional technical controls to try to avoid this situation in the future. |

# Measures Proposed to be Taken to Further Address the Breach

|  |
| --- |
| In addition we will be investing in advanced threat monitoring and detection software so that we will become aware of attacks on our infrastructure and can deal with them more effectively.  We will also be recruiting four further employees dedicated to maintaining our information security and that of the personal data we hold.  We intend to implement an Information Security Management System (ISMS) and gain certification to the ISO/IEC 27001 standard for information security within the next twelve months.  We intend to write to all of the data subjects involved and we will be offering all affected parties free fraud monitoring services for a period of two years. |

# Reasons for Delay in Notification, if applicable

|  |
| --- |
| Not applicable. |

# Guidance Notes for Completion

This form is intended to be used by an employee of Defradar Technologies to notify the supervisory authority of a breach of personal data in accordance with the requirements of the European Union General Data Protection Regulation (GDPR).

Correct use of this form, including where it should be sent to and how, is described in the document *Personal Data Breach Notification Procedure*.

**Name**

The name of the person that is officially submitting the personal data breach notification to the supervisory authority. This may be the Data Protection Officer or another (usually senior) employee of the organization.

**Title**

The role title of the submitter e.g. Data Protection Officer, Chief Information Officer

**Organization Name**

The official name of the organization submitting the notification.

**Organization Address**

The main address of the organization, to which correspondence about the personal data breach should be directed.

**Phone number**

The phone number(s) of the main contact point concerning the breach.

**Email Address**

The email address(es) of the main contact point concerning the breach.

**Date and Time Notification Submitted**

The date and time at which the notification is recorded as having been submitted. This should be completed shortly before the actual submission and maybe be overruled by the actual date and time of receipt by the supervisory authority.

**Date and Time of Detection of the Data Breach**

The date and time at which it was reasonably recognized by the organization that a breach affecting personal data occurred, or was highly likely to have occurred.

**Elapsed Time Between Detection and Notification**

The elapsed time, in hours, between the data breach having been recognized or detected by the organization and the personal data breach notification being submitted to the supervisory authority.

# Description of the Nature of the Personal Data Breach

Describe the nature of the personal data breach, including, where possible:

1. Categories and approximate number of data subjects concerned
2. Categories and approximate number of personal data records concerned

The description should include the current understanding of how the breach occurred (e.g. unauthorized access, accidental) and any supporting information.

# Likely Consequences of the Data Breach

A description of what the likely effects on data subjects may be of the breach and the risks they may face, including potential timescales.

# Measures Already Taken to Address the Breach

Describe the actions that have been taken prior to the notification to lessen the impact of the breach, stop any further breaches and otherwise address the risk to data subjects.

# Measures Proposed to be Taken to Further Address the Breach

Describe the further actions that have been identified, but not yet taken, that may help to lessen the impact of the breach, stop any further breaches and otherwise address the risk to data subjects.

# Reasons for Delay in Notification, if applicable

The GDPR requires that breaches of personal data that may result in a risk to the rights and freedoms of natural persons are notified to the supervisory authority without undue delay and, where feasible, not less than 72 hours after having become aware of it. If this timescale has not been met, the reasons for this should be stated here.