Personal Data Breach Notification Form

Notification Details

Name:	Roland Costea
Title:	CEO
Organization Name:	Defradar Technologies
Organization Address:	Piata Presei 3-5, Bucharest, Romania
Phone number:	+40 0723 344 546
Email Address:	rcostea@testradar.com

Date and Time Notification Submitted:	*05 Mar 2018 10:00*
Date and Time of Detection of the Data Breach:	*03 Mar 2018 18:00*
Elapsed Time Between Detection and Notification:	*40 hours*

Description of Personal Data Breach

An unpatched vulnerability in a module of our website software that was communicating with our backend database exposed an attacker to access confidential customer records and download them to an unauthorised computer via the Internet.

We believe that approximately 150.000 records have been accessed, consisting of customer names, addresses, social security numbers, email addresses and dates of birth for approximately the same number of data subjects, located in the Romania, Italy, Spain, UK and Bulgaria.

Impact

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

Steps taken

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.

Next steps

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.

Delay notifications

Not applicable.

How to use this document

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 Personal Data Breach

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

   a. *Categories and approximate number of data subjects concerned*

   b. *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.

Impact

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

Steps taken

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.

Next steps

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.

Delay Notifications, 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.