Data Protection Impact Assessment (DPIA)

January 2019

Contents

1. Processor

Processor Name	Phishing Tackle Limited
Registered Address	International House 24 Holburn Viaduct London EC1A 2BN
Contact Name	James Houghton
Contact Email	jamesh@phishingtackle.com
Position	CEO

2. Our Supervisory Authority

Information Commissioner's Office,
Water Lane,
Wycliffe House
Wilmslow
Cheshire SK9 5AF
international.team@ico.org.uk
+44 1625 545 745
www.ico.org.uk

3. Assessment Header

Project	Phishing Tackle
Project Description	Integrated Simulated Phishing, Information & Cyber Security Training, Breach Intelligence software platform.
Project Phase	Released / Production
Next DPIA Review	30 June 2019

4. General Information

Summary description of the project/initiative, including systems, applications, processes and data involved	Cloud based simulated email phishing, information and training software platform. Business email and organisational data is provided by the Controller.

Briefly describe the scope of the DPIA and any potential risks	The scope covers, but is not limited to, the electronic processing and storage by the Processor of personally identifiable information (PII) in the form of email addresses, full names, associated departments & employee numbers. The primary risk would be a compromised data storage or data processing server.
Who in the organisation will be responsible for processing the personal data once live	All processing is carried out electronically with no interaction or requirement for access to the data by any other party apart from the Data Controller.
The processing will involve sensitive personal data	No sensitive personal information is processed (as per definition of "Sensitive personal information" under The GDPR)

5. Assessment Details

5.1 Why do we need the DPIA

- Processing will result in evaluation or scoring, including profiling and predicting, especially from aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements.

5.2 Lawful basis which apply to the processing – Article 6.

- Processing is necessary for the purposes of the legitimate interests pursued by the controller

5.3 Legitimate interests by the Processor with regards to the processing.

- The processing of employee (or other authorised associates) behaviour data for cyber and information security analysis and training.

6. Data Subjects

What type(s) of data subjects are involved	Employee (or authorised agents) of Data Controller
How many data subjects are involved?	Governed by the Data Controller
Are data subjects in 1 Member Stateor spread	Governed by the Data Controller

7. Personal Data

What types of personal data will be collected and used?	Email addresses, Full Name, Employee Reference, Telephone Number, IP Address, Approximate Geographical Location data in the form of Longitude

	and Latitude based on IP address.
What types of sensitive personal data will be collected and used?	None
Will data be collected directly from data subjects, from third parties, or a combination of the two?	Provided by Data Controller
Will this be new data, existing data or a combination?	New
Will this involve the personal data of children or other vulnerable individuals such as the sick, elderly or handicapped? - describe	No
Where will the data be (1) processed, (2) stored, (3) analysed, (4) integrated	All data is will be processed, stored, analysed and integrated within Amazon Web Services located within the UK or EU, or USA depending on the Data Controller's geographical preference.
Storage periods for the categories of personal data	Data will be stored until the Data Controller wishes to terminate their contractual arrangement with Phishing Tackle Limited. At which time all data will be erased within 7 working days.

8. Processing

8.1 Purposes or reasons for processing the personal data

- Personal data will be used to conduct simulated email phishing campaigns. This process requires the email address, and other personal data listed herein, to be used for targeting and customising of such emails and their contents which are lawfully sent to the authorised recipients. Recipient pattern behaviour analysis is subsequently utilised to create training material and provide reporting based on for recipient progress and usage.

8.2 Intended data flows

Sources of the data, including from existing systems or other projects	Data will be either manually entered, imported from an external file or automatically collected via software synchronisation. All data will be lawfully provided by, and with the legal consent of the Data Controller.
Destinations of the data, including to existing systems or other projects	All data will be stored in electronic form within a database, or databases, solely controlled by Phishing Tackle Limited.
Describe any data protection relationship with, or dependency on other existing or planned projects	None
Describe where the data will be used in processing	All data will be consumed via the internet over an

once in production?	encrypted SSL connection.
Where will the data be stored when not in use?	All data will remain within the Phishing Tackle databases stored in their appropriate Amazon Web Services geographical location.
Name and country of any data processors involved in the project or in live processing operations	Phishing Tackle Limited, United Kingdom
Name and country of other recipients of the data	Controlled by the Data Controller
The country of any employees that may be involved with processing that is internal to the Processor.	United Kingdom
Once in production, how long will the data be retained before being deleted?	Data will be retained until such times as the contractual obligation between Phishing Tackle Limited and the Data Controller have terminated. After this period, all data will be permanently deleted within 7 working days.
Will the data be archived?	No

9. Risk Assessment

The processor shall consult the supervisory authority prior to processing, where a data protection impact assessment indicates that the processing would result in a high risk, in the absence of measures taken by the controller to mitigate the risk.

The Processor has embarked on a program of compliance with the GDPR and this initiative will provide for all data subjects' rights in the GDPR, including the provision of data subjects' access to their personal data and the proper response to and management of any breaches	✓ (SAR managed by Data Controller, where applicable)
The Processor complies with any related codes of conduct as stipulated in Article 40 of the GDPR	✓
The data involved has been (will be) kept to a minimum and will only be used for the purpose/s for which they were collected	✓
The appropriate storage periods will be applied to the purposes for processing and related personal data categories	✓
Where existing personal data is to be used, data subjects have been (or will be informed) if the processing is for a purpose other than for which the data was originally collected	✓
Where existing personal data is to be used, if the processing is for a purpose other than for which the data was originally collected, where necessary we will seek data subjects' consent	✓
Data subjects who have previously object to receiving direct marketing messages will be excluded from any campaigns associated with this initiative	✓

Notification to data subjects (privacy notices) will be optimised to include any information which is relevant to the new processing	✓
For any new processing, the relevant notification and associated consent or objection mechanisms will be provided at the points of collection	✓
Contracts and agreements between the controller and/or other recipients of the personal data, will be optimised accordingly	✓
Throughout its lifecycle, (collection, use, disclosure, storage and demise), the new processing activity will be incorporated into data protection practices (confidentiality, integrity; availability)	✓
Existing data protection practices will not be compromised by the introduction of the new processing	✓
Profiling will not be done on children's personal data	✓
The controller's legitimate interests will not override those of data subjects	✓
Any archived data will be pseudonymised	✓
Involved staff will be suitably trained on the new data protection requirements	✓
The relevant safeguards will apply where the data is to be transferred outside the EU (BCRs; 'adequacy' countries; model contracts)	✓