Managed Services Data Protection Impact Assessment Guidance

PHX068

Introduction

Data Protection Impact Assessments (DPIAs) are a management tool designed to identify any risks to a person's privacy when implementing new systems, technologies or process changes.

This document has been created by Phoenix Software to aid customer organisations to complete DPIAs on the procurement of a Phoenix Software Managed Service and identify any risk to the rights and freedoms of data subjects.

The use of the term "individuals" in this document refers to the holding of personal data for any customer individual consuming the service.

KEY DATA PROTECTION IMPACT ASSESSMENT INFORMATION

DPIA FAQ's

Data Protection Impact Assessment FAQ's	**Yes/ No**
Will the service itself involve the profiling, tracking, monitoring, evaluating, screening or making predictions about individuals in general, their performance, movement, behaviour or location?	**NO**
Will the service be collecting or involving special category personal data e.g. medical, health disability, criminal convictions/offences, children, vulnerable individuals, sexual orientation, ethnicity, religion, trade union association, political opinion, sexual orientation or financial information?	**NO**
Will the service be monitoring publicly accessible places for example CCTV?	**NO**
Will the service involve the use of technologies, digital solutions or Internet of Things (IoT) to process or store information for example, cloud-based systems?	**YES**
Will the service be processing biometric information e.g. fingerprints?	**NO**
Will the service be collecting or using information that individuals have providedto someone else and may not be aware is being shared with us?	**NO**
Will the service be monitoring or collecting information online (website) or otherdigital means for example, cookies or other online technical mechanisms?	**NO**
Will the service be using automated decision processing for example, a technical machine or algorithm is determining an outcome rather than a human intervention?	**NO**

Purpose

What information Phoenix Software need to collect for the Managed Service	Phoenix managed services act as an extension of the customer internal IT department. Technical environment information is provided by the customer to Phoenix to enable the managed service to be provided. Environment information can be shared at contract commencement or throughout the contracted period. End users requiring technical support via a managed service may provide technical information about a customer's environment to support the investigation and diagnostic process. Any Personal Data communicated is business owned by the customer organisation and may include information offered through email signature, including name, email, contact information and organisation.
What geographical areas does the data processing cover	The location of data processing varies depending on the managed service being provided. Please see below for a breakdown of service offerings, supporting toolsets and processing locations.
Who is the data subject	The Data Subject is the direct consumer of the service and the individuals involved in the procurement stages; therefore it is likely the data subject is the staff member of your organisation. This may differ per customer as the service may also process personal data relating to any Data Subject's of your organisation.

Nature

Who in Phoenix will have access to the data?	Phoenix operates the Principle of Least Privilege and Role Based Access Control. Access to the customer environment is limited to the service provisioning technical staff only – our IT Service Desk personnel. The allocated Customer Account and Success Managers have access to the customer organisation support, request and task tickets to provide additional support and context in the event of ticket escalation.
What hardware, software, networks, and/or paper systems will be used to collect or store the data?	Data including customer contact information; contract data; managed service scheduled tasks and review schedule is held with the Phoenix internal contract management system. Please see below for toolset breakdown.
How often will the data be used?	Data will be used as required by the service. The data will be updated into the performance dashboard daily. This will include the ticket requester name.

Data Minimisation

What measures are in place, or proposed, to ensure that only a minimum of data is collected, created, or obtained to enable Phoenix Software to proceed with Phoenix Software project?	Data held is restricted to that required to deliver the contract and that provided by individuals to raise support tickets. Due to the nature of the managed services provided by Phoenix, our service delivering staff members may have remote access to the customer environments. It is the responsibility of the customer to ensure that the access rights of Phoenix staff within the customer environments is proportionate and appropriate for service delivery.

Data Accuracy

What measures are in place, or proposed, to ensure that the data remains accurate and up-to-date?	Data held includes environment information which is updated through the course of the support contract. Customer contact information is updated as advised by the customer.

Data retention and disposal

What measures are in place, or proposed, to ensure that personal data collected, created, or obtained, will be kept for as short a period as possible?	In order to run the service, we only collect information relevant to the service and nothing more. Any data processed on your Data Subject's is supported in accordance with your requirements.
What retention periods are applied to the personal data?	Customer contact information is held for the contract duration +7 years. Any data belonging to your data subject's is deleted in accordance with your retention schedules and deleted upon service termination in accordance with our contract with you.
How will the data be treated at the end of the retention period?	Sensitive data destruction takes place as appropriate across systems.

Involvement of External Organisations

Managed Service	Supplier	Function	Data type	Data location
Reactive	ZenDesk	Support Ticketing Tool only	Support ticket content	Ireland
	Microsoft – PowerBI	Service Performance reporting – internally developed	Phoenix performance data; customer environment data fed from ZenDesk	UK
Proactive	ZenDesk	Support Ticketing Tool only	Support ticket content	Ireland
	Microsoft – PowerBI	Service Performance reporting – internally developed	Phoenix performance data; customer environment data fed from ZenDesk	UK
Patching	ZenDesk	Support Ticketing Tool only	Support ticket content	Ireland
	Microsoft – PowerBI	Service Performance reporting – internally developed	Phoenix performance data; customer environment data fed from ZenDesk	UK
Azure Essentials	ZenDesk	Support Ticketing Tool only	Support ticket content	Ireland
	Microsoft – PowerBI	Service Performance reporting – internally developed	Phoenix performance data; customer environment data fed from ZenDesk	UK
	VMware – CloudHealth	Cloud Management Platform Tool only	Cloud environment data including metadata	US
	Site 24x7	Infrastructure monitoring tool only	Availability metrics	US
AVD Essentials	ZenDesk	Support Ticketing Tool only	Support ticket content	Ireland
	Microsoft – PowerBI	Service Performance reporting – internally developed	Phoenix performance data; customer environment data fed from ZenDesk	UK
	VMware	CloudHealth – Cloud Management Platform Tool only	Cloud environment data including metadata	US

	Site 24x7	Infrastructure monitoring tool only	Availability metrics	US
Sentinel Essentials	ZenDesk	Support Ticketing Tool only	Support and event ticketcontent	Ireland
	Sentinel	Viewing platform for analysts	Analytics rules Automation Operational information	UK
	Microsoft -Lighthouse	Access platform	Functional only	UK
	Microsoft - PowerBI	Service performance reporting – internally developed	Phoenix performance data; customer environment data fed from ZenDesk	UK

The service itself will only collect the below data in order to operate:

Name, Address, Phone, Email	✔	Location	✔
Financial	✘	Disabilities	✘
Medical/Health	✘	Biometric or genetic	✘
Behavioural	✘	Profiling	✘
Criminal offences/convictions	✘	Photographic	✘
CCTV images	✘	Religious Beliefs, Trades Union Membership or Political Opinions	✘

Lawful Basis

For personal data being processed on your staff we process this data under a legitimate interest in order to manage the relationship with you. Any personal data on your data subject's being processed is based on your grounds for processing where we are acting as your processor.

Managing Risk

Phoenix is ISO27001 certified with no clause exclusions. This information security management standard ensures company focus on the confidentiality, integrity, and availability of information through technical controls, audit focus and risk management. Our ISO27001 Management system is audited twice annually by third party assessors.

To ensure appropriate focus of the risk management of the Management Services; Phoenix opted to become ISO20000 certified and achieved the certification in February 2020.

Version Control

Author	Version	Date	Description
Ben Rayner	1.0	01/08/2020	Original
Ben Rayner	2.0	01/08/2021	Revisions following review
Amy Trimble	3.0	27/01/2022	Includes Sentinel guidance

Document Approval

Name	Version	Date	Position
Sam Mudd	1.0	01/08/2020	Managing Director
Sam Mudd	2.0	01/08/2021	Managing Director
Sam Mudd	3.0	27/01/2022	Managing Director

Signed: _____Samantha Mudd, Managing Director

Dated: 22nd January 2022