Data Protection Policy

PHX086

Contents

Phoenix Software process Personal Data either for its own purposes, or on behalf of other entities (our customers). The company is therefore required under the Data Protection Act 2018 (DPA 2018), otherwise referred to as the UK General Data Protection Regulation (UKGDPR), to ensure that Personal Data is adequately protected. Our Data Protection Policy sets out our commitment to protecting personal data and how we implement that commitment with regards to the collection, protection, and use of that data.

We are committed to:

- ensuring that we comply with the data protection principles as listed below
- meeting our legal obligations as laid down by the UKGDPR
- ensuring that data is collected and used fairly, lawfully, and transparently
- processing personal data only in order to meet our operational needs or fulfil legal requirements
- taking steps to ensure that personal data is up to date and accurate
- ensuring that data subjects' rights can be appropriately exercised
- providing adequate security measures to protect data
- ensuring that a nominated officer is responsible for monitoring data protection compliance and provides a point of contact for all data protection issues
- ensuring that all staff are made aware of good practice in data protection and providing training if necessary
- ensuring that everyone handling personal data knows where to find further guidance
- ensuring that queries about data protection both internal and external to the organisation, are dealt with effectively and promptly
- regularly reviewing data protection procedures and guidelines

Data Protection Principles

Under the UKGDPR , the data protection principles set out the main responsibilities. We have summarised them for you as follows:

a) Personal Data should be used fairly (in relation to the individual who the data is about), lawfully (in accordance with UK laws) and honestly (ensuring we are transparent with the individual about what we're doing with their data).
b) Personal Data should be used only for explicit and clear purposes and where we have told the individual we will use it for one thing, we cannot simply use it for other things without checking first.
c) Personal Data should be adequate and limited to what is necessary for our purpose. If we don't need someone's Personal Data, why are we using it?
d) Personal Data should be accurate and, where necessary, kept up to date.
e) Personal Data should be kept no longer than is necessary. If we don't need it anymore, why are we keeping and maintaining it?
f) Appropriate controls should be in place to protect the Confidentiality, Integrity, and Availability of the Personal Data we hold.

g) Personal Data should be handled in an accountable manner and we all should be able to demonstrate that we are handling that data in accordance with these principles

Information Security

As a business, Phoenix Software Ltd holds Personal Data, about employees, customers, and vendors. It is imperative that this information is stored in a secure environment, used in a confidential manner, and only made available to relevant personnel.

For more information on how to handle information securely, please read the Information Security Policy.

Responsibilities

The Information Security Committee has day-to-day responsibility for data protection and security risks. Technical security for all sensitive information is the responsibility of Chief Technology Officer (CTO) and the IT team. Anyone suspecting a security breach must report it to the Information Security Committee immediately by e-mailing ISC@phoenixs.co.uk or by contacting a member of the committee.

All employees are responsible for making sure personal data is not compromised and that it is handled in accordance with the principles. Everyone who comes into contact with information about individuals or the business must be sure they understand how the data protection principles affects the way they deal with that information.

Everyone must read this Policy carefully and make sure that they, and others who work for us, comply with it. All employees are taken through this policy as part of the induction process, and all have continual access to this and other policies via SharePoint and the Company Handbook.

Any breach of data protection laws or security measures could have serious consequences. Any failure to comply with this policy will be treated as a disciplinary matter and may lead to summary dismissal.

Criminal Offences Under The Data Protection Act 2018

Data Protection is everyone's responsibility. Under the UKGDPR, however, if the organisation is found non-compliant with the law the organisation may be liable for any enforcement action taken.

Where individual members of staff cause a Personal Data breach or other serious Data Protection issue, it will be handled in accordance with the Company Handbook. Where any of the following has occurred, staff should be aware that these are specific criminal offences that can result in criminal prosecution under the DPA 2018.

1. Deliberately accessing or stealing personal data
2. Reidentifying anonymous data
3. Deleting Personal Data in order to prevent disclosure

The company must also maintain a registration with the Information Commissioner's Office (ICO). This is overseen by the Governance Manager. To view our registration, you can search online under the reference Z4809807.

Training and Awareness

Everyone is responsible for ensuring that they complete their Data Protection and Information Security training. Additionally, if you require additional support or training for your role, ensure that you contact the Governance Manager who will liaise with you on your specific need.

Version Control

Author	Version	Date	Description
Trevor Hutchinson	1.0	01/11/2019	Original Document
Trevor Hutchinson	2.0	01/11/2020	Amendments following annual review
Jane Singleton	3.0	01/11/2021	Amendments following annual review
Amy Trimble	3.0	05/12/2022	Annual review – no changes

Document Approval

Name	Version	Date	Position
Sam Mudd	1.0	01/11/2019	Managing Director
Sam Mudd	2.0	01/11/2020	Managing Director
Sam Mudd	3.0	01/11/2021	Managing Director
Clare Metcalfe	3.0	05/12/2022	Operations Director

Signed:  Clare Metcalfe, Operations Director

Dated: 05/12/2022