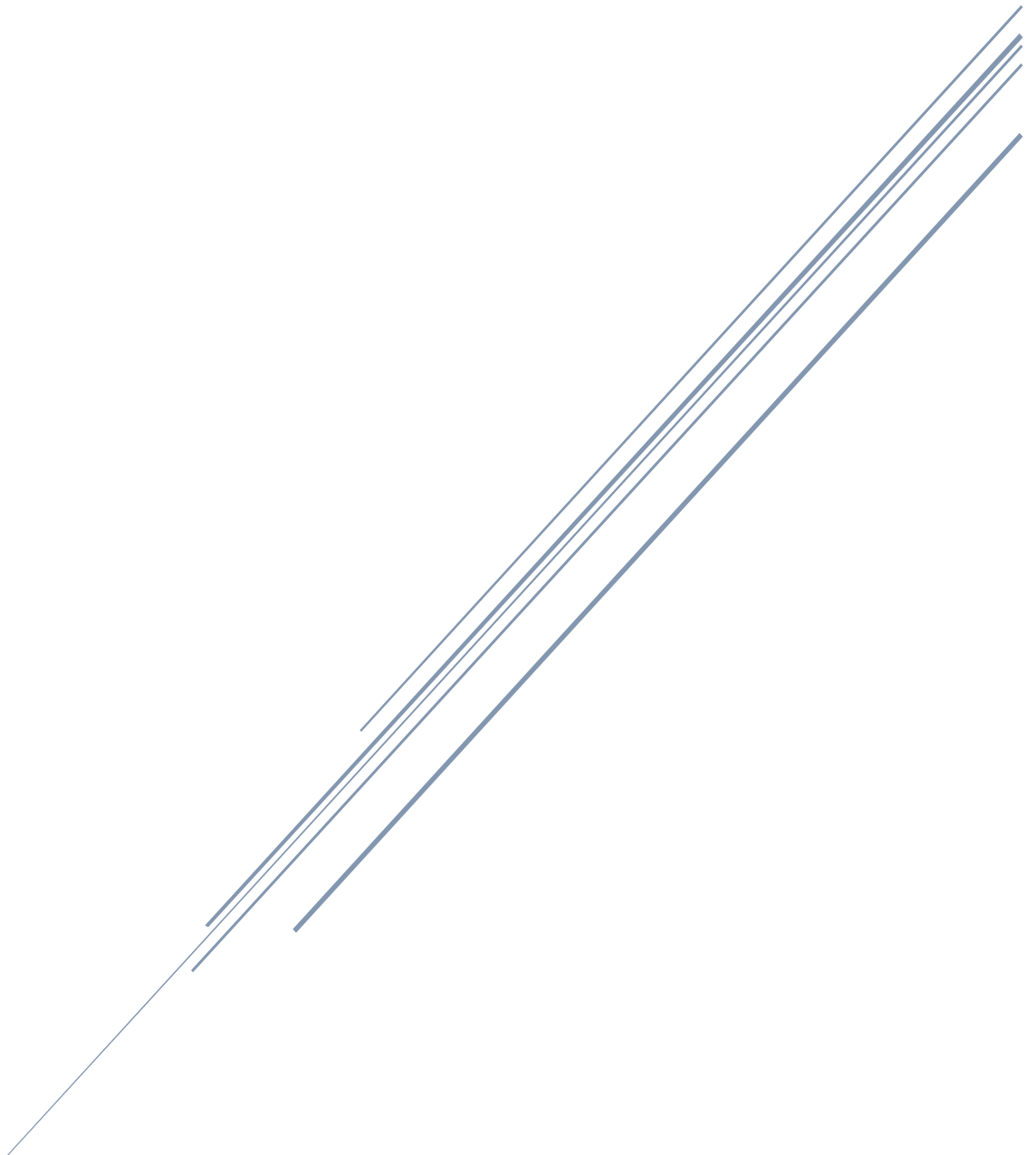




Hazard 360 Ltd Security Risk Management, Security Training, GDPR Compliance

# Data Protection Policy

DPP / PLY - 001



**Document Control:**

This document is valid for a period of 12 months from the date of issue and will be subject to an annual revalidation review by Hazard 360 Ltd.

Amendments will only be made with the approval Alan Smith Director. All amendments will be recorded in the tables below.

**Document Status:**

Document Reference	Hazard Legal Policies - Statements
Document Title	Data Protection Policy
Reference Number	DPP / PLY 001
Status	Live
Section No / Pages	7/7
Date Developed	01 / 01 / 2021
Author	Alan Smith
Approved By	Alan Smith
Owned by	© Hazard 360 Ltd

**Revision History**

Reference	Date	Revision	Summary Changes
DPP / PLY 001	01/01/2022	Alan Smith	Policy Review – No Change

## Contents

Document Control:.....	1
Document Status:.....	1
Revision History.....	1
1: Introduction.....	3
2: Purpose of Policy.....	3
3: Scope of Policy.....	3
4: Data Protection Act 2018 and GDPR 2018 Principles.....	4
Principle 1. Lawfulness, fairness, and transparency.....	4
Principle 2. Purpose limitations.....	4
Principle3. Data minimisation.....	4
Principle 4. Accuracy.....	4
Principle 5. Storage limitations.....	4
Principle 6. Integrity and confidentiality.....	4
5: Data Protection Risks.....	5
6: Responsibilities.....	5
6.1 Key Areas of Responsibility:.....	5
7: General Staff Guidelines.....	5
8: Data Storage.....	6
9: Data Use.....	7
10: Data Accuracy.....	7
11: Subject Access Requests.....	7
11.1 Subject Access Process – Protocols.....	8
12: Disclosing Information for Other Reasons.....	8
13: Providing Information.....	8

Data Protection Policy	Hazard 360 Ltd	Version: DPP / PLY / 001
Approved By: Alan Smith	Director – Hazard 360 Ltd	Version Date: 1 <sup>st</sup> Jan 2022
Security Classification: Internal	Page 2 of 8	Review Date: 1 <sup>st</sup> Jan 2023

## 1: Introduction

Hazard 360 Ltd needs to gather and use certain information about individuals.

These can include customers, business contacts, employees, and other people that Hazard 360 Ltd has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled, and stored to meet the company's data protection standards, and to comply with the law.

## 2: Purpose of Policy

The purpose of this policy is to ensure:

- Complies with the data protection law and follow good practice
- Protects the right of staff, customers, and associates
- Is open about how it stores and processes individual's data
- Protects itself from the risk of data breach

## 3: Scope of Policy

This policy applies to:

- The offices of Hazard 360 Ltd
- All contractors, suppliers, customers, and associates

It also applies to all data that Hazard 360 Ltd holds relating to identifiable individuals, even if that information technically falls outside of the Detection Protection Act 1998 and GDPR regulations.

This can include:

- Name of Individuals
- Postal Address
- Email Address
- Telephone Numbers

Data Protection Policy	Hazard 360 Ltd	Version: DPP / PLY / 001
Approved By: Alan Smith	Director – Hazard 360 Ltd	Version Date: 1 <sup>st</sup> Jan 2022
Security Classification: Internal	Page 3 of 8	Review Date: 1 <sup>st</sup> Jan 2023

## 4: Data Protection Act 2018 and GDPR 2018 Principles

The Data Protection Act 2018 and GDPR 2018 describes how organisations, including Hazard 360 Ltd must collect, handle and store personal information.

These rules Apply regardless of whether data is stored electronically, on paper or on other materials

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

### Principle 1. Lawfulness, fairness, and transparency<sup>1</sup>

Transparency: Tell the subject what data processing will be done.

Fair: What is processed must match up with how it has been described.

Lawful: Processing must meet the tests described in GDPR (Article 5, clause 1(a)).

### Principle 2. Purpose limitations<sup>2</sup>

Personal data can only be obtained for “specified, explicit, and legitimate purposes” (Article 5, Clause 1(b)). Data can only be used for a specific processing purpose that the subject has been made aware of, and no other, without further consent.

### Principle 3. Data minimisation<sup>3</sup>

Data collected on a subject should be “adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed” (Article 5, Clause 1 (c) i.e. No more than the minimum amount of data should be kept for specific processing.

### Principle 4. Accuracy<sup>4</sup>

Data must be “accurate and, where necessary, kept up to date” (Article 5, Clause 1 (d)).

Base lining ensures good protection and protection against identity theft. Data holders should build rectification processes into data management / archiving activities for subject data.

### Principle 5. Storage limitations<sup>5</sup>

Regulator expects personal data is “kept in a form which permits identification of data subjects for no longer than necessary” (Article 5, Clause 1 (e) i.e. Data no longer required should be removed.

### Principle 6. Integrity and confidentiality<sup>6</sup>

Requires processors to handle data “in a manner [ensuring] appropriate security of the personal data, including protection against unlawful processing or accidental loss, destruction or damage” (Article 5, Clause 1(f))

---

<sup>1</sup> GDPR Article 5 Clause (1a)

<sup>2</sup> GDPR Article 5 Clause (1b)

<sup>3</sup> GDPR Article 5 Clause (1c)

<sup>4</sup> GDPR Article 5 Clause (1d)

<sup>5</sup> GDPR Article 5 Clause (1e)

<sup>6</sup> GDPR Article 5 Clause (1f)

Data Protection Policy	Hazard 360 Ltd	Version: DPP / PLY / 001
Approved By: Alan Smith	Director – Hazard 360 Ltd	Version Date: 1 <sup>st</sup> Jan 2022
Security Classification: Internal	Page 4 of 8	Review Date: 1 <sup>st</sup> Jan 2023

## 5: Data Protection Risks

This policy helps protect Hazard 360 Ltd from some very real data security risks including:

### Breaches of Confidentiality:

Information being given out inappropriately or inadvertently

### Failing to Offer Choice:

All individuals should be free to choose how the Hazard 360 Ltd using data related to them

### Reputational Damage:

Hazard 360 Ltd could suffer if Hackers successfully gained access to sensitive data

## 6: Responsibilities

Everyone who works for or with Hazard 360 Ltd has some responsibility for ensuring data is collected, stored, and handled appropriately.

Persons who handle personal data must ensure that it is handled and processed in line with this policy and data protection principles.

### 6.1 Key Areas of Responsibility:

#### Board of Directors:

The board of directors is ultimately responsible for ensuring that Hazard 360 Ltd meets its legal obligations

## 7: General Staff Guidelines

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally, when access to confidential information is required, employees can request it from their line managers.
- Hazard 360 Ltd will provide training to all employees to help them understand their responsibilities when handling data.
- Employee should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, strong passwords must be used and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within the Hazard 360 Ltd or externally.
- Data should be regularly reviewed and updated if it is found to be out of date, if no longer required, it should be deleted and disposed of.
- Employees should request help from their line manager or the Data Protection Officer if they are unsure about the aspect of data protection.

Data Protection Policy	Hazard 360 Ltd	Version: DPP / PLY / 001
Approved By: Alan Smith	Director – Hazard 360 Ltd	Version Date: 1 <sup>st</sup> Jan 2022
Security Classification: Internal	Page 5 of 8	Review Date: 1 <sup>st</sup> Jan 2023

## 8: Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Data Controller.

Where data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason.

- When not required, the paper or files should be kept in a locked drawer or filing cabinet, or secure safe.
- Employees should make sure paper and printouts are not left where unauthorised people could see them, i.e. like on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.
- Where data is stored electronically, it must be protected from unauthorised access, accidental deletion, and malicious hacking attempts.
- Data should be protected by strong passwords, that are changed regularly and never shared between employees
- If data stored on removable media like (CD, DVD, or USB, Portable Drives) these should be kept locked away securely when not in use. (Where possible portable media should be encrypted)
- Data should only be stored on designated drives and servers and should be uploaded to an approved Cloud Computing Service.
- Servers containing personal data should be sited in a secure location away from general office space
- Data should be backed up on a daily basis. Those backups should be tested regularly, in line with Hazard 360 Ltd standard backup procedures
- Data should never be saved directly onto to laptops or other mobile devices like tablets, IPAD's or smart telephones.
- All servers and computers containing data should be protected by approved security software and a firewall.

Data Protection Policy	Hazard 360 Ltd	Version: DPP / PLY / 001
Approved By: Alan Smith	Director – Hazard 360 Ltd	Version Date: 1 <sup>st</sup> Jan 2022
Security Classification: Internal	Page 6 of 8	Review Date: 1 <sup>st</sup> Jan 2023

## 9: Data Use

Personal Data is of no value to Hazard 360 Ltd unless the business can make use of it, However it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption, or theft.

- When working with personal data, employees should ensure that the screens of their computer are always locked when left unattended.
- Personal data should not be shared informally. In particular it should never be sent by email, as this form of communication is not secure.
- Data must be encrypted before transferring electronically
- Personal data should never be transferred outside the European Union Economic Area
- Employees should never save copies of personal data to their own computers

## 10: Data Accuracy

The law requires Hazard 360 Ltd to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort Hazard 360 Ltd should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept accurate and as up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated, by confirmation of data on a regular basis.
- Hazard 360 Ltd will make it easy for data subjects to update the information Hazard 360 Ltd holds about them, this can be achieved via [www.hazatrd360ltd.com](http://www.hazatrd360ltd.com) web site.
- Data should be updated as inaccuracies are discovered.

## 11: Subject Access Requests

All individuals who are the subject of personal data held by Hazard 360 Ltd are entitled to:

- Ask what information Hazard 360 Ltd holds about them and why
- Ask how to gain access to information being held
- Be informed how to keep it up to date
- Be informed how Hazard 360 Ltd is meeting its data protection obligations

Data Protection Policy	Hazard 360 Ltd	Version: DPP / PLY / 001
Approved By: Alan Smith	Director – Hazard 360 Ltd	Version Date: 1 <sup>st</sup> Jan 2022
Security Classification: Internal	Page 7 of 8	Review Date: 1 <sup>st</sup> Jan 2023



### 11.1 Subject Access Process – Protocols

- If an individual contacts Hazard 360 Ltd requesting information, this is call a “**Subject Access Request**”
- Subject access requests from individuals should be made by using the contact page on Hazard 360 Ltd website ([www.hazard360ltd.com](http://www.hazard360ltd.com)) the data controller shall supply a “Subject Access Request Form” to the individual making the request.
- Individuals will be charged £10.00 per subject access request. The data controller is to supply the information within 14 days upon receipt of the subject access request form.
- The data controller will always verify the identity of anyone making a subject access request before handling over any information.

## 12: Disclosing Information for Other Reasons

In certain circumstances, the Data Protection Act 1998 allows personal data to be disclosed to law enforcement agencies without consent of the data subject

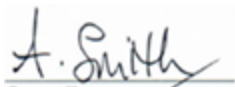
Under these circumstances, Hazard 360 Ltd will disclose requested data, however the data controller must ensure that the request is legitimate.

## 13: Providing Information

Hazard 360 Ltd aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the Data is being used
- How to exercise their rights

To these ends Hazard 360 Ltd has a privacy statement setting out data relating to individuals is used by Hazard 360 Ltd. This statement is available to view on the Hazard 360 Ltd website site under the privacy tab.



Alan Smith

Director

Hazard 360 Ltd

Data Protection Policy	Hazard 360 Ltd	Version: DPP / PLY / 001
Approved By: Alan Smith	Director – Hazard 360 Ltd	Version Date: 1 <sup>st</sup> Jan 2022
Security Classification: Internal	Page 8 of 8	Review Date: 1 <sup>st</sup> Jan 2023