DATA CLASSIFICATION POLICY

1. Policy introduction

Here at THEHEALTHCHECK LTD, we are committed to data security, the privacy of the individual and upholding all our compliance obligations under GDPR. We take our responsibilities seriously, and we recognise that the use of information assets and data form a crucial aspect of our business activity. That is why we've devised the following Data Classification Policy to outline the way in which we classify and use data.

Our Data Classification Policy is designed to ensure that:

- THEHEALTHCHECK LTD adheres to all necessary legal obligations
- We implement controls to maximise return on investment
- THEHEALTHCHECK LTD maintains availability, confidentiality and integrity where necessary for all data
- Our company has the ability to chart data protection levels that protect both THEHEALTHCHECK LTD as well as the individuals whose personal data we must collect, process or store
- We are able to avoid threats of disclosure and/or unauthorised access to data

2. Policy values

Data classification is a vital process our company must carry out to ensure the individuals who claim a legitimate right to access information we hold are able to do so. Our data classification process must also ensure our data and any other piece of information we hold is protected from any and all individuals or organisations that should not have access to that information.

THEHEALTHCHECK LTD's Data Classification Policy identifies and elaborates upon the correct handling and classification processes our company must use, as per the regulatory requirements that we:

- Make data available to all those individuals who have a legitimate reason to access it
- Manage all data in line with its corresponding classification
- Maintain the integrity of all data
- Ensure all data our company holds is accurate, complete and consistent

3. Policy objectives

THEHEALTHCHECK LTD's Data Classification Policy has been developed to meet the following objectives:

- To outline the duties and responsibilities of THEHEALTHCHECK LTD employees that ensure data is kept safe and secure
- To establish a robust data classification process that is consistent and compliant with UK regulatory requirements
- To ensure data is sufficiently protected and encrypted so that unwarranted actions will not be taken against THEHEALTHCHECK LTD in the event data is lost, damaged or accessed illegally
- To avoid and minimise reputational or operational damage to THEHEALTHCHECK LTD, our stakeholders, clients, customers or partners associated with compromised data

4. Policy implementation

To make sure our Data Classification Policy is effective, THEHEALTHCHECK LTD will implement the following procedures:

- All users of data will be identified and provided access to data in which they have a legitimate need to access
- All data will be classified, managed and controlled in relation to its correct categorisation, as per the processes and requirements outlined within this policy
- THEHEALTHCHECK LTD must ensure control mechanisms are created and implemented to protect data we collect, process or store
- All control mechanisms and classification protocols must be reviewed and amended as required by law on a regular basis
- Data users and data controllers must implement and maintain adequate levels of physical security as required, in relation to computer facilities or access terminals from which data can be viewed or accessed
- THEHEALTHCHECK LTD must ensure that all data and relevant equipment is safely disposed of, as and when required

5. Obligations under GDPR (2018) and Data Protection Act 2018 (DPA)

THEHEALTHCHECK LTD is committed to meet its regulatory obligations under GDPR and DPA. That is why we are committed to ensure that adequate and appropriate measures are taken to prevent the unauthorised access or illegal processing or storage of data. We are required to do everything we can, within reason, to protect the data we use and hold against destruction, accidental loss or damage.

6. Data classifications

Data that is sensitive in nature must be adequately protected at all times. To properly assign safeguards, all data that our company collects, processes or stores must be assigned one of the following classification categories:

- Public
- Open
- Confidential
- Strictly Confidential
- Secret

A vast amount of the data THEHEALTHCHECK LTD uses will most likely be classed as being either 'Public' or 'Open' data. Any information relating to an individual or organisation that could identify them or is personal or private in nature must be assigned a category of either 'Confidential' or 'Strictly Confidential'.

This is to ensure THEHEALTHCHECK LTD upholds its regulatory commitment to uphold the rights of individuals, as outlined under GDPR.

On rare occasions, THEHEALTHCHECK LTD may wish to class data as 'Secret'. If an employee is unsure as to whether they should categorise a piece of data as being secret – or if they need assistance in classifying any other piece of data, they should consult a line manager. If no manager is available for consultation, data should default to a 'Confidential' classification.

7. Data classification types and handling procedures

To minimise discrepancies and ensure THEHEALTHCHECK LTD does everything it can to uphold its regulatory commitments, the following working definitions should be associated with the aforementioned classification categories.

Public data

Public data is information or data that can be accessed by any external individual or organisation.

Types of public data might include:

- Official contact data of relevant company employees
- News updates or press releases
- Company publications
- External-facing company policies or procedures

How to handle public data:

Public data should be formatted to allow for the most basic security measures. Examples might include converting a Word document into a PDF to avoid others editing it, as this could subsequently cause some form of reputational damage.

Open

Anyone is able to access this information.

Types of open data might include:

- Official contact data e.g. full name, primary email address and telephone number
- Authorised communications, such as blogs, news articles and industry updates
- Approved company policies, guidance and processes

How to handle open data:

Open data should be formatted to allow for the most basic security measures. Examples might include converting a Word document into a PDF to avoid others editing it, as this could subsequently cause some form of reputational damage.

Confidential data

Access to confidential data must be limited only to individuals who have been granted appropriate authorisation to view or process that information.

Alternatively, there may be occasions in which unauthorised individuals or stakeholders may need to be granted access to confidential data; however, this access must only be provided on a need-to-know basis.

Types of confidential data might include:

- Someone's personal details or any information that could be used to identify them. Examples of identifiable or personal details include:
  - Name
  - Date of birth
  - Address
  - Telephone number

    - Email address
    - National Insurance number
    - Race
    - Religion
    - Health details
    - Political affiliations
    - Trade union membership
    - Criminal offences
- Employee contracts
- Non-Disclosure Agreements
- Unfinished or unapproved company documents
- Employee wage slips
- Death certificates
- PDR documentation

How to handle confidential data:

As and where required to handle confidential data, employees should exercise the following handling processes:

- Paper documents must be:
    - In secure locked storage
    - Transported in sealed envelopes only
    - Transported by an approved third-party courier service
    - Securely disposed of

- Electronic data must be:
    - Encrypted
    - Password-protected wherever possible
    - Transportation must follow secure file transfer protocol
    - Storage must be limited to secure file stores
    - Securely disposed of

Strictly confidential data

A minimal number of authorised individuals, authorities or other stakeholders may be permitted access to data that has been classified as being ‘Strictly confidential’.

Types of strictly confidential data might include:

- Bank details
- Credit card information
- Financial information
- Server information
- Usernames or passwords

- Test data
- Medical records
- Disciplinary proceedings
- Patent information
- Network information

How to handle strictly confidential data:

As and where required to handle strictly confidential data, employees should exercise the following handling processes:

- Paper documents must be:
  - In secure locked storage
  - Transported in sealed envelopes only
  - Transported by an approved third-party courier service

- Electronic data must be:
  - Encrypted
  - Password-protected wherever possible
  - Tagged
  - Transportation must follow secure file transfer protocol
  - Storage must be limited to secure file stores

Secret data

Access to data that has been classed as 'Secret' or a request to access secret data is subject to the Official Secrets Act.

Various types of secret data may require different controls and circumstances. Bearing that in mind, individual protocols should be reviewed on a case-for-case basis in line with UK Government requirements. Government advice concerning the handling of secret data should be sought.

8. Data classification markings

Data classification markings need to be clearly visible at all times and must match the classification category in which that data has been assigned. Appropriate data classification identification markings should be included either at the top, bottom or centre of each document page.

9. Reclassifying data

There may be occasions in which data must be reclassified from one data category to another

data category. The need for reclassification could depend upon a content change, or an alteration in terms of the data's intent, where it is stored or how it is being used. Before reclassifying data, a firm and justifiable rationale must be established. If in doubt, contact the Data Protection Officer or your line manager for guidance.

10. Sensitive data

It is the responsibility of the data owner or the data originator to define the category of data classification for a piece of data. Responsibility also rests with the data owner or originator to ensure that adequate protection has been afforded to that data in line with its relevant classification.

Any data that could or should be defined as being personal in nature must be afforded a higher level of protection and be treated as data that is sensitive. Personal data can be classed as information relating to an individual that could identify them. Aforementioned examples of sensitive personal data might include (among other pieces of data) a person's name, contact information, race, religion, political affiliations, sexual preference and so on.

Sensitive data must be identified and assessed on a case-for-case basis. In most cases, sensitive data will inherently be classed as confidential; thus, access and/or availability must be limited. Sensitive data which is made available in the public domain can lead to reputational damage for private individuals or company employees. As a company we must ensure that sensitive data is given sufficient protection to protect individuals, company employees and the company itself.

11. Data storage and backup

Because data is such an integral aspect of our business, it is everyone's responsibility at THEHEALTHCHECK LTD to do everything within their power to ensure that sensitive data is being collected, processed, backed up, stored and secured in line with company policy.

12. Data anonymisation

Prior to the sharing, transfer or disclosure of data, THEHEALTHCHECK LTD and its employees must take all necessary steps to ensure that the anonymity of corresponding data subjects is protected and maintained in line with our regulatory commitments.

Necessary steps may include omitting or redacting (deleting) said personal identifiers within a piece of data. Audio visual data or verbally exchanged data recordings should be likewise edited.

13. Secure data disposal

Sensitive data that is no longer needed or has reached an ‘end of life’ classification as decided upon by the relevant authorised individuals must be disposed of in a secure fashion. Examples of disposing data as stored on paper would include shredding.

14. Data security response

If data is damaged or lost, it must be immediately reported to an appropriate line manager and company Data Protection Officer, and logged as an incident requiring urgent response.