DATA SECURITY POLICY

Introduction

Here at THEHEALTHCHECK LTD, we collect, process and store personal data for a range of business purposes. Data subjects include customers, suppliers, partners, employees, clients and other stakeholders and individuals.

Bearing in mind THEHEALTHCHECK LTD's commitment to uphold the rights of the individual as enshrined in law, our data security policy is designed to protect all past, current and future employees, customers, or partners, from illegal or damaging activity conducted by others using their personal data.

Our data security policy outlines how THEHEALTHCHECK LTD will endeavour to guard and protect all personal data. It also sets out to raise the awareness of staff members in relation to the ways in which GDPR impacts their use of individual's personal data.

This policy applies to all data processing activities involving THEHEALTHCHECK LTD, and includes activities or systems related to both internal business operations, as well as external relations and any third-party agreements.

Please note that THEHEALTHCHECK LTD's data security policy applies to all employees, and this policy may be subject to review and amendment on a regular basis. For more information about this policy and its overall implementation, consult our Data Protection Officer.

This document is subject to regular review to ensure ongoing regulatory compliance.

Data security policy definitions

Personal data

Personal data encompasses any type of information that relates to an identifiable individual. Various types of personal data THEHEALTHCHECK LTD may collect, store and process could include:

- Contact details
- Financial information
- Educational background
- Certifications
- Skills
- Nationality
- Marital status
- Job title

The above list is by no means exhaustive, and should be used merely as a point of reference from which a working definition of personal data can be established and further developed.

Sensitive personal data

Under GDPR, sensitive personal data is defined as encompassing any of the following:

- Racial or ethnic origin
- Political opinion
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data
- Health-related information
- Sexual orientation

It is paramount that all sensitive personal data is kept under stringent control as part of the implementation of our data security policy.

Purposes of personal data

THEHEALTHCHECK LTD uses personal data for a range of various purposes. These purposes may include:

- Financial
- Administrative
- Human resources
- Regulatory compliance
- Payroll

- Business development

Please note the above list is by no means exhaustive, and should merely be used as a reference point from which a working definition of purpose can be established.

Business purposes

THEHEALTHCHECK LTD must carry out a range of functions and processes as part of our operational activity. Data kept in relation to these activities falls under the category of data for business purposes, which includes information of the following nature:

- Operational
- Compliance
- Policy adherence
- Human resources and personnel
- Marketing

The above list is by no means exhaustive, and should be used merely as a point of reference from which a working definition of business purposes can be established and further developed.

Fair processing

At THEHEALTHCHECK LTD, there will be occasions when employees will need to process personal data; however, processing activities must always be carried out in a fair and lawful manner that is compatible with the rights of each corresponding individual. Consequently, we should avoid processing the personal data of any individual who has not provided us with explicit consent.

Our company must strive to obtain explicit consent at all costs, and we must clearly identify to the individual what data is being processed, why we need to use it and who will have access to their data. These factors must be identified and clearly reiterated to the individual at the point of request for consent.

It's worth noting there may be exceptional circumstances in which we are asked to process sensitive personal data without consent. An example of an exceptional circumstance could include legal obligations we may need to carry out to comply with health and safety regulations.

THEHEALTHCHECK LTD endeavours to take all actions necessary to ensure that all personal data we obtain, process and store is accurate, relevant and adequate in relation to the reason in which we asked for that information. We should not hold excessive or irrelevant data on any individuals, and we will not process any personal data for a purpose unrelated to the purpose in which the relevant individual has consented to the processing of their data.

Our roles and responsibilities

Data security is a critical component of our business. It falls on everyone at THEHEALTHCHECK LTD to take responsibility for data security, and all employees must familiarise themselves with our data security policy and do everything within their power to uphold that policy on a day-to-day basis.

Please note that THEHEALTHCHECK LTD takes data protection incredibly seriously, and we expect all staff members to adhere to this data security policy. Any failure and refusal to comply with this policy could ultimately place our company at risk.

Bearing that in mind, personal non-compliance with this data security policy could lead to disciplinary action as they relate to ordinary personnel procedures. Please contact your line manager with any further questions concerning data protection at THEHEALTHCHECK LTD.

As a staff member at THEHEALTHCHECK LTD, you can expect to receive data protection training in line with our data security policy. All incoming employees will be provided training as an aspect of the wider staff induction process, and all staff members can anticipate the requirement to undergo additional training as a result of subsequent regulatory updates to GDPR or other relevant legislation as it relates to data security.

Data security will inevitably encompass a range of additional responsibilities for various roles within the company. These roles and their responsibilities include (but are not limited to):

Data Protection Officer

GDPR stipulates our company must appoint a Data Protection Officer. It is our Data Protection Officer's responsibility to:

- Organise data security training for all employees not specifically referenced within this data security policy.
- Review and analyse all existing data security protocols and processes on a regular basis.
- Be a point of contact for all employees, clients and stakeholders to answer questions about data protection and data security.
- Respond to internal or external queries from individuals wanting to know what data relating to them may have been obtained, processed or stored by our company.
- Conduct due diligence and submit approval in relation to any contractual agreement with a third party involving the processing or storage of data.
- Maintain constant contact with company directors, board members and stakeholders in relation to data security, company responsibilities and data risk management.

IT Manager

Information technology plays a crucial role in the way our company operates. Any processes relating to IT and the processing and storage of data must be carefully monitored, assessed and guided by an IT Manager.

It is the responsibility of THEHEALTHCHECK LTD's IT Manager to:

- Conduct due diligence and appropriate levels of research into any third-party service that our company may call upon to store or process any data.
- Make sure that all company software, IT systems, equipment and services meet changing levels of data security standards.
- Carry out regular checks, audits and scans to ensure security hardware and security software are fully functional and optimised to manage and mitigate data security risks.

Marketing Manager

A significant proportion of our marketing activities involve the collection, storage and processing of data. Consequently, our Marketing Manager must oversee the following responsibilities:

- Accept all queries relating to data security and data protection from leads, media outlets, clients or other individuals and oversee and deliver an adequate response.
- Work alongside THEHEALTHCHECK LTD's Data Protection Officer to make sure that all of our marketing processes, campaigns and activities are compliant with all relevant data security and data protection laws – as well as our own company data security policy.
- Review, draft and approve any relevant data security statements that must accompany emails, other messages or applicable marketing collateral.

Our data security policies

THEHEALTHCHECK LTD takes data security extremely seriously, and we place the rights of the individual and regulatory adherence at the heart of everything we do as a company.

In light of our commitments, it is mandatory all staff members must observe and adhere to the following data security policies:

Data storage policy

- All information or data that is collected and processed is subject to all of the applicable requirements as outlined and documented within this policy. This includes information collected electronically, by paper, telephone or data collected through any other means.
- All data must be collected, stored and protected in a secure location appointed by THEHEALTHCHECK LTD, for a retention period as predefined by corresponding legislature or company policy.
- Staff members are strictly forbidden to retain confidential information or personal data not relating to themselves on their personal devices. Exceptions to this policy include information that is needed for a purpose that is work-related, temporary and specified and approved by a relevant manager.
- Staff members should avoid downloading sensitive files or confidential information to local devices wherever possible. Information being necessarily processed for work purposes may be exempt from this policy.
- Employees must install and use software and systems that have been licensed and approved by the company on devices while carrying out the duties of their role. Downloading or using any software, app or system that is not preapproved by the company will require prior approval from the company's IT Manager.
- All mobile and portable devices used by staff members should be approved by the company's IT Manager and secured to prevent unauthorised access or breach. Personal devices could include a laptop, smartphone, tablet or any other handheld computing devices. This policy also applies to any shared cloud storage spaces.
- All internet access and online operations carried out by employees could be subject to monitoring and filtering in accordance with relevant legislation and company policy. This monitoring should be carried out only by the IT Manager or an authorised member of staff.
- Employees must adhere to all applicable elements of this policy when using personal devices to access company resources. Similarly, employees must observe and adhere to all applicable elements of this data security policy when using equipment provided by THEHEALTHCHECK LTD to access information externally.
- Employees are forbidden from using public access devices. This practice is allowed in some circumstances; however, prior and explicit approval from a line manager for regular public access must be obtained and recorded.

- Employees must use access tools provided to them by a client or partner of THEHEALTHCHECK LTD if access is granted to any third-party storage system or data storage facility.
- It is forbidden to send, forward or submit any of the information or data referred to within this data security policy to a third-party unless deemed essential to complete approved processes.
- If an employee needs to carry out an approved submission of data to any relevant third-party, that data must be made secure in accordance with company policy and any relevant third-party data protection protocols.

Please note that THEHEALTHCHECK LTD will carry out regular system audits to monitor and ensure ongoing compliance with this data security policy and all regulatory requirements as outlined under GDPR.

Data retention policy

While THEHEALTHCHECK LTD must routinely collect and store data, we are committed to the rights of individuals. That's why we retain all information and personal data for no longer than we need to.

The necessary length of retention will often be decided on a case-for-case basis, bearing in mind the rationale and original purpose surrounding data collection and retention. Decisions of this nature must be made in a way that is compatible with our existing data retention guidelines under GDPR.

For additional guidance, consult the following corresponding documents:

- Data retention and erasure policy document

International data transfer policy

Employees must observe a series of restrictions that apply towards the international transfer of data or personal information. Employees are not permitted to transfer personal information or data outside of the United Kingdom without having obtained explicit permission in the first instance from the company's Data Protection Officer.

Data encryption and anonymisation policy

THEHEALTHCHECK LTD deploys encryption to secure and protect data that is stored on devices from unlawful processing or unauthorised access. Encryption is also used to protect information that is in transit.

We also use the anonymisation of personal data wherever deemed prudent to ensure the rights of the individual are fully protected and observed.

In line with these principles, we are committed to the use both encryption and anonymisation as a risk management tool alongside existing systems, to protect the company from accidental

loss, as well as from the damage or destruction of data or personal information.

Activities that are prohibited

Unless otherwise noted or informed, employees are strictly forbidden from using company equipment, tools or systems for any purpose unrelated to their role responsibilities, excluding any previously mentioned exceptions. This policy also relates to any relevant systems, tools or equipment belonging to a company client or partner.

Bearing that in mind, the following activities should be deemed forbidden with no exceptions:

- Any unauthorised replication of copyrighted materials.
- The violation of individual rights by way of the unnecessary collection, storage and processing of personal data or information.
- The violation of rights of an individual or organisation protected under intellectual property law in any jurisdiction.
- The use of any programme, command or interface designed to interfere with a user or corresponding user session.
- The accessing of any data, user account or server for any purpose unrelated to the business function of an individual's company role.
- Issuing fraudulent product or service offers from a company account.
- The allowed sharing or use of employee login credentials or company systems by anyone apart from the named individual.
- The export of proprietary or confidential information as it relates to the company.
- The export of any software or data that is in breach of regulation or the company's data security policy.
- Knowingly causing a network disruption or security breach.
- An employee is not allowed to access data that is not intended for them by logging into a system or gaining access to a confidential or limited-access account. The only exception to this rule is if the employee is granted access as part of a specific company project.

Please note that any violation of this policy can lead to disciplinary action, alongside legal action where deemed prudent or necessary.

Reporting security issues

If you encounter any incidents or issues relating to the security or protection of information or data, you must report this immediately to company management. Management will subsequently take and record any action deemed necessary to prevent damage or loss in relation to a security threat.

If necessary, it is the responsibility of company management to report relevant incidents relating to a data breach or information security threat to regulators or the authorities. Under GDPR, it also falls upon management to contact the individuals involved in any breach or security threat.