Introduction

Nudge Global Limited needs to gather and use certain information about individuals.

These can include customers, suppliers, business contacts, employees and other people that the organisation 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.

Why this Policy exists

This data protection policy ensures that Nudge Global Limited:

- Complies with data protection law and follows good practice.
- Protects the rights of staff, customers and partners.
- Is open about how it stores and processed individual's data.
- Protects itself from the risks of a data breach.

Data Protection Law

The General Data Protection Regulations (GDPR) describes how organisations, including Nudge Global Limited, must collect, handle and stored 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. Additionally, the legislation provides for several rights of the individuals which are outlined in this document, and this policy describes how to deal with these rights.

The GDPR is underpinned by several important principles. These say that personal data must:

1. Be processed fairly, lawfully and transparently.

2. Be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

3. Be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

4. Be accurate and kept up to date, inaccurate data should be amended as soon as possible.

5. Not be held for any longer than necessary.

6. Processed in accordance with the rights of data subjects.

7. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection.

People, Risks & Responsibilities

Policy Scope

This policy applies to:

- The head office of Nudge Global Limited.
- All branches of Nudge Global Limited.
- All staff and volunteers of Nudge Global Limited.
- All contractors, suppliers and other people working on behalf of Nudge Global Limited.

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act. This can include:

- Names of individuals.
- Postal addresses.
- Email address.
- Telephone numbers.
- Date of birth.
- Salary.
- Dependant's details.

Data Protection Risks

This policy helps to protect Nudge Global Limited from some very real data security risks, including:

- Breaches of confidentiality. For instance, information being given out inappropriately.
- Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them.

- Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with Nudge Global Limited has some responsibility for ensuring that data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The Board of Directors is ultimately responsible for ensuring that Nudge Global Limited meets its legal obligations.
- The Data Protection Officer (Peter Kovacs - Information Security Specialist) is responsible for:
    - Keeping the Board updated about data protection responsibilities, risk and issues.
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
    - Arranging data protection training and advice for the people covered by this policy.
    - Handling data protection questions from staff and anyone else covered by this policy.
    - Dealing with requests from individuals to see the data Nudge Global Limited holds about them (also called 'subject access requests').
    - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

- The IT Manager is responsible for:
    - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
    - Performing regular checks and scans to ensure that security hardware and software is functioning properly.
    - Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.

- The Marketing Director is responsible for:
    - Approving any data protection statement attached to communications such as emails and letters.
    - Addressing any data protection queries from journalists or media outlets like newspapers.
    - Where necessary, working with other staff to ensure that marketing initiatives abide by data protection principles.

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 manager.
- Nudge Global Limited will provide training to all employees to help them understand their responsibilities when handling data.
- Employees 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 company 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 Information Security Officer if they are unsure about any aspect of data protection.

Breach Reporting

In the event of a Breach of DPA, the Information Commissioners Office is notified in writing within 24 hours. The potential detriment to individuals is the overriding consideration in deciding whether a breach of data security should be reported to the ICO. Serious breaches would be notified to the ICO using the standard ICO DPA security breach notification form. All breach reporting will be done by the Information Security Officer

Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Information Security Officer.

When 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.
- Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.

When 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.
- As a general rule data should not be stored on removable media, and individual machines have been disabled to prevent the use of removable media. However, if on an exceptional basis, the Information Security Officer allows data to be stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers and should only 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 frequently. Those backups should be tested regularly in line with the company's standard backup procedures.
- Data should never be saved directly to laptops or other mobiles devices like tablets or smart phones.
- All servers and computers containing data should be protected by approved security software and a firewall.

Data Use

Personal data is of no value to Nudge Global Limited 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 the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally. It should never be sent by email, as this form of communication is not secure.
- Data must be encrypted before being transferred electronically.
- Personal data should never be transferred outside of the European Economic Area.
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.
- Any data received via email should be immediately transferred to a secure storage and the original email should then be permanently deleted from the email account. No client data should be retained in email folders.
- Any data that is downloaded by an individual should be saved to a secure location, data that is downloaded for temporary use must be permanently deleted from the download folder and the recycle bin at least monthly.

Data Accuracy

The law requires Nudge Global Limited to take reasonable steps to ensure that data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort Nudge Global Limited should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure that it is kept as accurate and 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 that data is updated. For instance, by confirming a employee's details when they call.
- Nudge Global Limited will have a policy for data subjects to update the information Nudge Global limited holds about them which is easily explained and accessible.
- Data should be updated as inaccuracies are discovered. For instance, if a employee can no longer be reached on their stored telephone number, it should be removed from the database.

Rights of the Individual (Data Subject)

GDPR provides for a number of rights that the individual has regarding their own data, this section outlines the policies for each of the rights.

Right to be informed

GDPR sets out the information that you should supply and when individuals should be informed.
The information supplied is determined by whether or not you obtained the personal data directly from individuals.

Much of the information required is consistent with current obligations under the DPA, but there is some further information you are explicitly required to provide.

The information you supply about the processing of personal data must be:

- concise, transparent, intelligible and easily accessible;
- written in clear and plain language, particularly if addressed to a child; and
- free of charge.

The information that Nudge Global Ltd provides to individuals is contained within our Data Privacy Notice. This is available on our corporate website at any time. In addition, individuals are advised of our Data Privacy Notice when we issue a welcome nudge to them. This is the first opportunity we have to provide the information. This privacy notice can also be found on the main landing page when an employee logs in.

Subsequent communication also has a reference to the Data Privacy Notice with a link to obtain further information.

An individual has the right to request this information by emailing Support@Nudge-Global.com and the request will be dealt with by the Information Security Officer.

Right of Access

All individuals who are the subject of personal data held by Nudge Global Limited are entitled to:

- Ask what information the company holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the company is meeting its data protection obligations.

If an individual contacts the company requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the Information Security Officer at Support@nudge-global.com. The Information Security Officer can supply a standard request form, although individuals do not have to use this.

The Information Security Officer will always verify the identity of anyone making a subject access request before handing over any information.

The information must be provided as soon as possible and at the latest within one month of the request being made.

As Nudge Global Limited are considered Data Processors for all of our clients, and subject access requests must first of all be referred to the client contact to obtain confirmation they are happy for us to provide the information. The client has the right to handle the subject access request directly with the individual should they wish to do so.

The right to rectification

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.

If personal data in question has been disclosed to third parties, we must inform them of the rectification where possible. You must also inform the individuals about the third parties to whom the data has been disclosed where appropriate.

As much of Nudge Global Ltd.'s data come from the employer, once notified of inaccurate data all steps must be taken not only to rectify the data within the Nudge

application, but also to inform the employer so that the source data is amended. If the data in question is related to additional information provided by the information, this can be remedied by the individual themselves.

In any event the rectification must be completed within one month of the request

Rectification requests should be made to Support@Nudge-Global.com and will be dealt with by the Information Security Officer.

The right to erasure (the right to be forgotten)

The right to erasure is also known as 'the right to be forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data whether there is no compelling reason for its continued processing.

The right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal data erased and to prevent processing in specific circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed (i.e. otherwise in breach of the GDPR).
- The personal data has to be erased in order to comply with a legal obligation.
- The personal data is processed in relation to the offer of information society services to a child.

Where personal data is disclosed to third parties, you must inform them about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

The right to erasure of data being used for the provision of Financial Education can take two forms.

- The right to have data removed completely from the application (also known as the right of erasure); we will remove the details from our application and delete the data stored on the application. We will also advise the employer that this right has been exercised so that no further personal data is received. This does mean that the individual will no longer be able to take part in the service and they won't receive Financial Education in the future.
- The right to unsubscribe; in this instance, we will ensure that the individual does not receive any communication from us in the future, however the details will continue to be stored on our application and we will receive data updates

from the employer. The individual will still be able to take advantage of the Financial Education materials in the application but will no longer received proactive education.

To exercise these rights an individual must email Support@Nudge-Global.com providing employee ID, employer name and the nature of the request. For the avoidance of doubt:

- A request for removal will result in the data being completed deleted. However, this must be explicit and clear that all data is to be removed.
- Any other request will result in the unsubscription from the notification service and data will not be deleted.

Erasure requests will be dealt with by the Information Security Officer.

The right to restrict processing

When processing is restricted, we are permitted to store the personal data, but not further process it. We can retain just enough information about the individual to ensure that the restriction is respected in future.

- We will be required to restrict the processing of personal data in the following circumstances:
- Where an individual contests the accuracy of the personal data, you should restrict the processing until you have verified the accuracy of the personal data.
- Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and we are considering whether your organisation's legitimate grounds override those of the individual.
- When processing is unlawful and the individual opposes erasure and requests restriction instead.
- If you no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.

The procedures for handling these requests are the same as the Right to Erasure and are dealt with in this section above.

The right to data portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.

It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

We must provide the personal data in a structured, commonly used and machine-readable form. This can be done as a csv or excel file.

Requests to receive data in a portable manner should be made to Support@Nudge-Global.com and will be dealt with by the Information Security Officer.

Requests must be completed within one month of receipt of the request.

The right to object

- Individuals have the right to object to:
  processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics

Individuals must have an objection on "grounds relating to his or her particular situation".

We must stop processing the personal data unless:

- We can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
- the processing is for the establishment, exercise or defence of legal claims.

We must inform individuals of their right to object "at the point of first communication" and in your privacy notice.
This must be "explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information".

Requests which are exercising the right to object should be made to Support@Nudge-Global.com and will be dealt with by the Information Security Officer.

Rights related to automated decision making and profiling

The GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention.

Individuals have the right not to be subject to a decision when:

- it is based on automated processing; and
- it produces a legal effect or a similarly significant effect on the individual.

In these circumstances individuals must be able to:

- obtain human intervention;
- express their point of view; and
- obtain an explanation of the decision and challenge it.

Whilst the Nudge application does provide information which could be considered People Like You, this information does not have a legal or similar effect and therefore

in general terms this right does not apply, particularly as no decisions are made based on this data. However if an individual requests information regarding the amount and type of profiling that is done by the Nudge application, this should be treated in the same way as a Data subject request and efforts should be made to explain the process that is applied.

Requests of this type should be made to Support@Nudge-Global.com and will be dealt with by the Information Security Officer.

Disclosing Data for Other Reasons

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

Under these circumstances, Nudge Global Limited will disclose requested data. However, the Information Security Officer will ensure the request is legitimate, seeking assistance from the Board and from company's legal advisers where necessary.

Providing Information

Nudge Global Limited 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, the company has a privacy statement, setting out how data relating to individuals is used by the company.