Data Protection Policy

UK Data Protection Act 2018 (Including UK General Data Protection Regulation (GDPR))

Note: This policy is to be reviewed at least annually from the publication of the last version.

Document Control **Version control / history**

Name	Description	Date
O'H	Version 1.0	22nd March 2018
O'H	Version 2.0	16th January 2019
O'H	Version 3.0	3rd March 2020
Fabian Roberts	V4.0	24 Feb 21
Fabian Roberts	V5.0	26 Jan 2022

Approvals

Name	Position	Date
Ted Jones	CEO	23rd March 2018
Ted Jones	CEO	18th January 2019
Ted Jones	CEO	10th March 2020
Ted Jones	CEO	24 Feb 21
Ted Jones	CEO	Jan 2022

This policy applies to all employees of Northcott Global Solutions and includes third parties, temporary, contract staff and anyone who comes into contact with the Northcott Global Solutions resources, sites, and properties that fall under the control of Northcott Global Solutions. It also applies to all current locations, and new locations shall take the policy into account during the design, development or feasibility of access control systems being installed in new construction or as part of any major or minor improvement project.
The above will be referred to as users in the rest of this document.
Note: that in cases where any applicable legal, statutory or other regulations for the protection or accessibility of corporate information / records exist, these may take precedence over this policy

Information and UK's Data Protection Act 2018 (DPA) 2018 Policy

Northcott Global Solutions Ltd is committed to the protection and privacy of personal data, including that provided by third parties, and is subject to the UK's Data Protection Act (DPA) 2018 and the principles of the EU General Data Protection Regulation (GDPR) it aligns to.

DPA 2018 covers the protection of natural persons regarding the processing of personal data, and the free movement of such data. It gives individuals greater rights over their personal information, and places greater obligations on organisations to protect this data. It includes the right to be forgotten, the right to know when personal data falls into the wrong hands and the need for explicit consent (in certain cases) prior to processing personal information.

The Primary Principle of GDPR - "Privacy by design and by default"

"Privacy by design and by default" stipulates that — from the initial stages onwards — organisations must consider the impact that processing and controlling personal data can have on an individual's privacy.

Accountability and compliance

Companies covered by the GDPR are rightly held more accountable for their handling of an individual's personal data. NGS takes its responsibilities in this regard extremely seriously – not only is it a legal requirement but it is also pivotal for client confidence in the company. All NGS staff are to adhere closely to its data protection policies, impact assessments and documentation covering regulatory requirements on how data is processed.

Personal data: Is "any information relating to an identified or identifiable natural person". Personal data can be anything that allows a living person to be directly or indirectly identified. This may be a name, an address, or even an IP address. It includes automated personal data and can also encompass pseudonymised data (e.g. nicknames) if a person can be identified from it.

Sensitive personal data: There are greater and more specific conditions to be satisfied for sensitive personal data (or 'special categories') of information. These include trade union membership, religious beliefs, political opinions, racial information, and sexual orientation.

There is also a requirement for businesses to obtain consent to process data in some situations. When an organisation is relying on consent to lawfully use a person's information they have to clearly explain that consent is being given and there has to be a "positive opt-in".

Controller: A controller is an entity that decides the purpose and manner that personal data is used or will be used.

Processor: The person or group that processes the data on behalf of the controller. Processing is obtaining, recording, adapting or holding personal data.

Requests for personal information are free-of-charge. When someone asks a business for their data, they must provide the information within one month. Everyone will have the right to get confirmation that an organisation has information about them, access to this information and any other supplementary information.

Lawful Basis for Processing Personal Data

Because NGS processes personal data, it must identify the lawful basis for its processing activity in the DPA 2018, document it and ensure the company's privacy notice is updated to explain it. It is vital that the company has legitimate grounds for data retention. As a principle, NGS will process personal data only to the extent that it is necessary to do so, and to do otherwise would dramatically impact NGS' ability to provide the best service to its clients.

There are six legitimate reasons for processing personal data:

(1) **Consent**– where the individual has given their clear consent for NGS to process their data for a specific purpose (see below)

(2) **Contract** – where it is necessary to process someone's personal data to fulfil contractual obligations to them; or because they have asked NGS to do something before entering into a contract (e.g. provide a quote).

(3) **Legal Obligation** – where it is necessary to process the personal data to comply with a common law or statutory obligation – this legal obligation must duly be defined.

(4) **Vital Interests** – where it is necessary to process the personal data to protect someone's life. NGS cannot rely on 'vital interests' for health data or other special category data if the individual is capable of giving consent, even if they refuse their consent.

(5) **Public Task** – where data processing is necessary for a company to perform a task in the public interest or for its official functions, and the task or function has a clear basis in law. It is unlikely

(6) **Legitimate Interests** - the most "flexible" lawful basis for processing data. There is a three- part test:

a. identify a legitimate interest;
b. show that the processing is necessary to achieve it; and
c. balance it against the individual's interests, rights and freedoms.

If NGS uses people's data in ways they would reasonably expect, and which have a minimal privacy impact, or where there is a compelling justification for the processing, then this basis works. The company will keep a record of all Legitimate Interests Assessments (LIAs).

Consent

NGS must keep a thorough record of how and when an individual gives consent to store and use their personal data.

Consent means **active** agreement e.g. a pre-ticked box isn't enough. As a company that controls how and why data is processed, NGS will have to show a clear audit trail of consent e.g. saved consent forms.

Individuals also have the right to withdraw consent at any time, which has to be easy, and they have the right to be forgotten, so their details must be permanently erased, and not just deleted from a mailing list. The CIO has ultimate responsibility for ensuring this work is carried out and guaranteed when requested.

Children

Where there is a potential need to process data relating to minors, NGS will verify individuals' ages and seek parental or guardian consent for any data processing activity.

Prepare for data security breaches

In the event of a breach, companies must inform the relevant authorities within 72 hours, giving full details of the breach and proposals for mitigating its effects. Monitoring protocols must be able to recognise and act on breaches as soon as they happen, and an incident recovery plan put in place to deal with the repercussions. NGS' Data Breach policy refers.

If you are a supplier to others, consider whether you have new obligations as a processor

The DPA 2018 imposes some direct obligations on processors which need to be understood and built into the company's policies, procedures and contracts. All client facing staff and those specifically involved in contracts must ensure that this documentation is up to date and adequate. The NGS Service Provider Network Manager must track this with such providers, in particular confirming with them what data processing services they may use, and that these do not conflict with NGS's own obligations.

Cross-border data transfers

In certain situations, it may be desirable to transfer data across borders. NGS must be clear that it has a legitimate basis for transferring personal data to jurisdictions that are not recognised as having adequate data protection regulation. This is not a new concern, but a failure to comply could attract a fine of up to the greater of EUR20m and 4% of annual worldwide turnover, so the consequences of non-compliance could be severe.

Compliance

NGS is mandated to meet the requirements of the UK's Data Protection Act 2018 and the GDPR that sits alongside this when processing personal data. As well as renewing our registration with the ICO annually, NGS:

- trains all staff to support the fair and lawful processing of personal data
- adheres to its Data Protection Impact Assessments
- implements security processes to prevent the unlawful disclosure of personal data
-

- implements retention and disposal processes to ensure information is retained only as long as necessary
- follows mandated reporting processes in the event of any breach.

Examples of Threats

Accidental data leaks

This is one of the most frequent sources of security breaches e.g. typing the wrong email address. A strong internal security policy is necessary, but it still might not be enough to avoid fines for a simple accident (and subsequent damage to reputation).

Disloyal employees

Disgruntled employees have taken advantage of weaknesses in internal processes and controls to take revenge against their organisation. Organisations need to have a solid data-access policy, data- classification tools that restrict access by user profile, identity and access management controls, and cyber-intelligence services to minimise this risk.

Cyber crime

The theft of personal information (e.g. via targeted malware) has become a profitable cybercrime. Organisations have to make sure their cyber defences can prevent data from falling into the wrong hands. An end-to-end approach is essential — each company has to protect against all potential risks.

Data Protection Policy Annexes:

Annex A	Privacy Notice Emergency Medical and Non-Medical	Public
Annex B	Privacy Notice Tracking and Travel Management	Public
Annex C	Privacy Notice Third Party Administrator	Public
Annex D	Privacy Notice Business Development	Public
Annex E	Privacy Notice NGS Employee	Internal
Annex F	Data Privacy Impact Assessment Medical and Non-Medical	Public
Annex G	Data Privacy Impact Assessment Tracking and Travel Management	Public
Annex H	Data Privacy Impact Assessment Third Party Administrator	Public
Annex I	Data Privacy Impact Assessment Business Development	Public
Annex J	Legitimate Interest Assessment Medical and Non-Medical	Internal
Annex K	Legitimate Interest Assessment Tracking and Travel Management	Internal
Annex L	Legitimate Interest Assessment Third Party Administrator	Internal
Annex M	Legitimate Interest Assessment Business Development	Internal
Annex N	Legitimate Interest Assessment Third Party Informants	Internal
Annex O i)	Release of Information Consent English	Internal
Annex O ii)	Release of Information Consent French	Internal
Annex O iii)	Release of Information Consent Spanish	Internal
Annex O iv)	Release of Information Consent German	Internal
Annex P	Data Subject Consent Form General	Public
Annex Q	Parental Consent Form	Public
Annex R	Parental Consent Withdrawal Form	Public
Annex S	Data Subject Consent Withdrawal Form General	Public
Annex T	Data Subject Access Request Form	Public
Annex U	Data Subject Access Request Procedure	Internal
Annex V	Data Subject Disclosure Form	Internal

Relevant Documentation:

Information Security Policy
Data Classification Policy
Information Retention Policy
Information Disposal Policy
ICO Certificate