Data Protection Policy

UK Data Protection Act 2018 (Including the EU's Regulations (GDPR)

Note: This policy requires 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

Approvals

Name	Position	Date
Ted Jones	CEO	23rd March 2018
Ted Jones	CEO	18th January 2019
Ted Jones	CEO	10th March 2020

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

22 Bevis Marks, London EC3A 7JB • +44 207 183 8910
info@northcottglobalsolutions.com • www.northcottglobalsolutions.com

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 2018 and the principles of GDPR therein. DPA 2018 covers the protection of natural persons with regard to the processing of personal data, and the free movement of such data. It gives citizens of EU countries greater rights over their personal information, and place 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 more accountable for their handling of an individual's personal data. It is for this reason NGS adheres to our data protection policies, data protection impact assessments and documents all 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's 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 can be made 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 stores personal data, we must identify the lawful basis for our processing activity in the DPA 2018, document it and update your privacy notice to explain it. It is vital that we have legitimate grounds for its retention.

That aside we must consider what data processing we undertake. Some instances will require a person's consent, for example, or we must show a legitimate interest in processing that data that is not overridden by the interests of that person? Companies often assume that they need to obtain a person's consent to process their data. However, consent is just one of a number of six ways of legitimising processing activity and may not be the best (e.g. it can be withdrawn):

(1) **Consent**–see below

(2) **Contract** - we need to process someone's personal data to fulfil our contractual obligations to them; or because they have asked us to do something before entering into a contract (e.g. provide a quote).

(3) **Legal Obligation** - we need to process the personal data to comply with a common law or statutory obligation. Wherein we must be able to identify the legal obligation.

22 Bevis Marks, London EC3A 7JB • +44 207 183 8910
info@northcottglobalsolutions.com • www.northcottglobalsolutions.com

(4) **Vital Interests** - if we need to process the personal data to protect someone's life. We 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) **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 you use 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. Keep a record of all Legitimate Interests Assessments (LIAs). Criminal Offence Data – to process personal data about criminal convictions or offences, you need to show one of the five bases above and either legal authority or official authority for the processing of such data.

Consent

Companies 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. Companies that control how and why data is processed 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.

Review how you seek, record and manage consent and whether you need to make any changes. If you do rely on obtaining consent, review whether your documents and forms of consent are adequate and check that consents are freely given, specific and informed. You will bear the burden of proof. Refresh existing consents now if they don't meet the DPA 2018 standard.

Children

Assess whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.

Prepare for data security breaches

Put in place clear policies to ensure that you can react quickly to any data breach and notify in time where required. 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.

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 you will need to understand and build into your policies, procedures and contracts. You are also likely to find that your clients will wish to ensure that your services are compatible with the enhanced DPA 2018 requirements. Consider whether your contractual documentation is adequate and, for existing contracts, check who bears the cost of making changes to the services as a result of changes in laws or regulations. If you obtain data processing services from a third party, it is very important to determine and document your respective responsibilities.

Cross-border data transfers

With any international data transfers, including intra-group transfers, it will be important to ensure that you have 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

Northcott Global Solutions Ltd is mandated to meet the requirements of the UK's Data Protection Act 2018 and the EU's General Data Protection Regulations when processing personal data. In order to fulfil its obligations under DPA 2018, Northcott Global Solutions Ltd has implemented robust practices and policies. As well as renewing our registration with the ICO annually, the Northcott Global Solutions Ltd trains all staff to support the fair and lawful processing of personal data, demonstrate our compliance by adhering to our Data Protection Impact Assessments, implements security processes to prevent the unlawful disclosure of personal data,

22 Bevis Marks, London EC3A 7JB • +44 207 183 8910
info@northcottglobalsolutions.com • www.northcottglobalsolutions.com

implements retention and disposal processes to ensure information is retained only as long as necessary and follow the 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. type 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.

22 Bevis Marks, London EC3A 7JB • +44 207 183 8910
info@northcottglobalsolutions.com • www.northcottglobalsolutions.com

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	February 2020
Data Classification Policy	February 2020
Information Retention Policy	February 2020
Information Disposal Policy	February 2020
ICO Certificate	2020

22 Bevis Marks, London EC3A 7JB • +44 207 183 8910
info@northcottglobalsolutions.com • www.northcottglobalsolutions.com