# Data Protection Policy - GDPR

This document can be made available in other formats, on request

Review date: 3rd February 2021
Next Review Date: 3rd February 2023

NIC SERVICES GROUP LTD

# Data Protection Policy – GDPR

**Introduction**

NIC Services Group Ltd (NIC) is a multi-services company that provides services to clients in the UK and EU.

The personal data that NIC processes to provide these services is related to their employees, clients, and other individuals as necessary.

NIC is committed to a policy of protecting the rights and privacy of individuals, including employees and others, in accordance with the General Data Protection Regulation (GDPR) May 2018.

NIC needs to process certain information about its employees and other individuals with whom it has a relationship for various purposes such as, but not limited to:

1. The recruitment and payment of employees.
2. The administration of T&A information.
3. Employee engagement and enrolment.
4. Employee training records and accreditations.
5. Recording employees progress, attendance, and conduct.
6. Complying with legal obligations to government including local government.

To comply with various legal obligations, including the obligations imposed on it by the General Data Protection Regulation (GDPR) NIC must ensure that all this information about individuals is collected and used fairly, stored safely and securely, and not disclosed to any third party unlawfully.

**Scope**

This policy applies to all personal data processed by NIC and is part of NIC's approach to compliance with data protection law. All employees are expected to comply with this policy. Any breach of this policy or of the Regulation itself will be considered an offence and the company disciplinary procedures will be invoked.

As a matter of best practice, other companies, agencies, and individuals working with NIC and who have access to personal information, will be expected to read and comply with this policy. It is expected that departments who are responsible for dealing with external bodies will take the responsibility for ensuring that such bodies sign a contract which among other things will include an agreement to abide by this policy.

This policy will be updated as necessary to reflect best practice in data management, security, and control and to ensure compliance with any changes or amendments to the GDPR and other relevant legislation.

**Data Protection Principles**

The legislation places a responsibility on every data controller to process any personal data in accordance with the eight principles. NIC Services Group Ltd is defined as the data controller. More detailed guidance on how to comply with these principles can be found at the ICO's website (www.ico.gov.uk)

In order to comply with its obligations, NIC undertakes to adhere to the eight principles:

1. **Process personal data fairly and lawfully.**
   NIC will make all reasonable efforts to ensure that individuals who are the focus of the personal data (data subjects) are informed of the identity of the data controller, the purposes of the processing, any disclosures to third parties that are envisaged; given an indication of the period for which the data will be kept, and any other information which may be relevant.

2. **Process the data for the specific and lawful purpose for which it collected that data and not further process the data in a manner incompatible with this purpose**.
NIC will ensure that the reason for which it collected the data originally is the only reason for which it processes those data, unless the individual is informed of and consents to any additional processing before it takes place.

3. **Ensure that the data is adequate, relevant, and not excessive in relation to the purpose for which it is processed.**
NIC will not seek to collect any personal data which is not strictly necessary for the purpose for which it was obtained. Forms for collecting data will always be drafted with this mind. If any irrelevant data is given by individuals, it will be destroyed immediately.

4. **Keep personal data accurate and, where necessary, up to date.**
NIC will review and update all data on a regular basis. It is the responsibility of the individuals giving their personal data to ensure that this is accurate, and each individual should notify NIC if, for example, a change in circumstances mean that the data needs to be updated. It is the responsibility of NIC to ensure that any notification regarding the change is noted and acted on.

5. **Only keep personal data for as long as is necessary.**
NIC undertakes not to retain personal data for longer than is necessary to ensure compliance with the legislation, and any other statutory requirements. This means NIC will undertake a regular review of the information held and implement a weeding process. NIC will dispose of any personal data in a way that protects the rights and privacy of the individual concerned (e.g. secure electronic deletion, shredding and disposal of hard copy files as confidential waste). A log will be kept of the records destroyed.

6. **Process personal data in accordance with the rights of the data subject under the legislation.**
Individuals have various rights under the legislation including a right to:
    - be told the nature of the information NIC holds and any parties to whom this may be disclosed.
    - prevent processing likely to cause damage or distress.
    - prevent processing for purposes of direct marketing.
    - be informed about the mechanics of any automated decision-making process that will significantly affect them.
    - not have significant decisions that will affect them taken solely by automated process.
    - sue for compensation if they suffer damage by any contravention of the legislation.
    - take action to rectify, block, erase or destroy inaccurate data.
    - request that the Office of the Information Commissioner assess whether any provision of the Act has been contravened.

    NIC will only process personal data in accordance with individuals' rights.

7. **Put appropriate technical and organisational measures in place against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of data.**
All employees are responsible for ensuring that any personal data which they hold is kept securely and not disclosed to any unauthorised third parties.
NIC will ensure that all personal data is accessible only to those who have a valid reason for using it.
NIC will have in place appropriate security measures and controlled access to all personal data and will put in place appropriate measures for the deletion of personal data. A log will be kept of the records destroyed.

This policy also applies to employees and others who process personal data 'off-site', e.g. when working at home, and in circumstances additional care must be taken regarding the security of the data.

8. **Ensure that no personal data is transferred to a country or a territory outside the European Economic Area (EEA) unless that country or territory ensures adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.**
   NIC will not transfer data to such territories without the explicit consent of the individual. This includes publishing of information on NIC's website and social media accounts. NIC will always seek the consent of individuals before placing any personal data on these platforms, including photographs.
   NIC will provide a clear and detailed privacy statement prominently on the website, and social media profiles.

**Consent as a basis for processing**

Although it is not always necessary to gain consent from individuals before processing their data, it is often the best way to ensure that data is collected and processed in an open and transparent manner.
Consent is especially important when NIC is processing any sensitive data, as defined by the legislation.
NIC understands consent to mean that the individual has been fully informed of the intended processing and has signified their agreement whilst being of a sound mind and without having any undue influence exerted upon them. Consent obtained based on misleading information will not be a valid basis for processing. Consent cannot be inferred from the non-response to a communication.

NIC will ensure that any forms used to gather data on an individual will contain a statement (fair collection statement) explaining the use of that data, how the data may be disclosed and also indicate whether or not the individual needs to consent to the processing.

NIC will ensure that if the individual does not give his/her consent for the processing, and there is no other lawful basis on which to process the data, then steps will be taken to ensure that processing of that data does not take place.

**Data Subject Rights**

NIC has processes in place to ensure that it can facilitate any request made by an individual to exercise their rights under data protection law. All employees have received training and are aware of the rights of data subjects. Employees can identify such a request and know who to send it to.

All requests will be considered without undue delay and within one month of receipt as far as possible.

**Subject access**: the right to request information about how personal data is being processed, including whether personal data is being processed and the right to be allowed access to that data and to be provided with a copy of that data along with the right to obtain the following information:

- the purpose of the processing
- the categories of personal data
- the recipients to whom data has been disclosed or which will be disclosed
- the retention period
- the right to lodge a complaint with the Information Commissioner's Office
- the source of the information if not collected direct from the subject, and
- the existence of any automated decision making

**Rectification**: the right to allow a data subject to rectify inaccurate personal data concerning them.

**Erasure**: the right to have data erased and to have confirmation of erasure, but only where:

- the data is no longer necessary in relation to the purpose for which it was collected, or
- where consent is withdrawn, or
- where there is no legal basis for the processing, or
- there is a legal obligation to delete data

**Restriction of processing**: the right to ask for certain processing to be restricted in the following circumstances:

- if the accuracy of the personal data is being contested, or
- if our processing is unlawful but the data subject does not want it erased, or
- if the data is no longer needed for the purpose of the processing but it is required by the data subject for the establishment, exercise or defence of legal claims, or
- if the data subject has objected to the processing, pending verification of that objection

**Data portability**: the right to receive a copy of personal data which has been provided by the data subject and which is processed by automated means in a format which will allow the individual to transfer the data to another data controller. This would only apply if NIC was processing the data using consent or on the basis of a contract.

**Object to processing**: the right to object to the processing of personal data relying on the legitimate interests processing condition unless NIC can demonstrate compelling legitimate grounds for the processing which override the interests of the data subject

**Procedure for review**

This policy will be updated as necessary to reflect best practice or future amendments made to the General Data Protection Regulation (GDPR) May 2018 and Data Protection Act 1998.

Please follow this link to the ICO's website www.ico.gov.uk which provides further detailed guidance on a range of topics including individuals' rights, exemptions from the Act, dealing with subject access requests, how to handle requests from third parties for personal data to be disclosed etc. You may find it helpful to read the Guide to Data Protection which is available from the website.

For help or advice on any data protection or freedom of information issues, please do not hesitate to contact: The Data Protection Officer (DPO): Krystal Simpson (ksimpson@nicgroup.co.uk, ext: 231)