# GDPR compliance statement

## Introduction

The **EU General Data Protection Regulation ("GDPR")** came into force across the European Union on 25th May 2018 and brought with it the most significant changes to data protection law in two decades. Based on privacy by design and taking a risk-based approach, the EU GDPR has been designed to meet the requirements of the digital age. Subsequently, upon leaving the EU, the **Data Protection Act 2018** was updated to enact the **UK GDPR**, replicating the EU GDPR.

The 21st Century brings with it broader use of technology, new definitions of what constitutes personal data, and a vast increase in cross-border processing.

The UK GDPR aims to standardise the regulation of data protection laws and processing across the UK, to work within the EU, as well as influence other legislation across the globe; affording individuals stronger, more consistent rights to access and control their personal information.

## Our commitment

At NetSupport we are committed to ensuring the security and protection of the personal information that we process, and to providing a compliant and consistent approach to data protection. We have always had a robust and effective data protection programme in place which complied with existing law and abides by the data protection principles. However, we recognise our obligations in updating and expanding this programme to meet the demands of the UK GDPR legislation.

We are dedicated to safeguarding the personal information under our remit and in developing a data protection regime that is effective, fit for purpose and demonstrates an understanding of and appreciation for the new Regulation. Our objectives and activities around GDPR compliance have been summarised in this statement and include the development and implementation of new data protection roles, policies, procedures, controls and measures to ensure maximum and ongoing compliance.

## How we have a GDPR-friendly culture

The NetSupport Group of companies has a consistent level of data protection and security across our organisation; however, it is our continued aim to have a culture that is fully compliant with the UK GDPR. Our actions include:

- **Information audit** – We carry out company-wide information audits to identify and assess what personal information we hold, where it comes from, how and why it is processed and if and to whom it is disclosed.
- **Policies and procedures** – **We r**evise data protection policies and procedures to meet the requirements and standards of the UK GDPR and any relevant data protection laws, including: -
    - **Data protection** – Our main policy and procedure document for data protection has been overhauled to meet the standards and requirements of the UK GDPR. Accountability and governance measures are in place to ensure that we understand and adequately disseminate and evidence our obligations and responsibilities; with a dedicated focus on privacy by design and the rights of individuals.
    - **Data retention and erasure** – We have updated our retention policy and schedule to ensure that we meet the 'data minimisation' and 'storage limitation' principles, and

that personal information is stored, archived and destroyed compliantly and ethically. We have dedicated erasure procedures in place to meet the new 'Right to Erasure' obligation and are aware of when this and other data subjects' rights apply, along with any exemptions, response timeframes and notification responsibilities.

  - **Data breaches** – Our breach procedures ensure that we have safeguards and measures in place to identify, assess, investigate and report any personal data breach at the earliest possible time. Our procedures are robust and have been disseminated to all employees, making them aware of the reporting lines and steps to follow.
  - **International data transfers and third-party disclosures** – Where NetSupport Ltd stores or transfers personal information outside the EU, we have robust procedures and safeguarding measures in place to secure, encrypt and maintain the integrity of the data. Our procedures include a continual review of the countries with sufficient adequacy decisions, as well as provisions for binding corporate rules; standard data protection clauses or approved codes of conduct for those countries without. We carry out strict due diligence checks with all recipients of personal data to assess and verify that they have appropriate safeguards in place to protect the information, ensure enforceable data subject rights and have effective legal remedies for data subjects where applicable.
  - **Subject Access Request (SAR)** – We are revising our SAR procedures to accommodate the revised 30-day timeframe for providing the requested information and for making this provision free of charge. Our new procedures detail how to verify the data subject, what steps to take for processing an access request, what exemptions apply and a suite of response templates to ensure that communications with data subjects are compliant, consistent and adequate.

- **Legal basis for processing** - – We have reviewed all processing activities to identify the lawful basis for processing and ensuring that each basis is appropriate for the purpose it relates to. Where applicable, we also maintain records of our processing activities, ensuring that our obligations under Article 30 of the UK GDPR and Schedule 1 of the Data Protection Act are met.
- **Privacy Notice/Policy** – We have revised our Privacy Notice(s) to comply with the UK GDPR, ensuring that all individuals whose personal information we process have been informed of why we need it, how it is used, what their rights are, who the information is disclosed to and what safeguarding measures are in place to protect their information.
- **Obtaining consent** - – We have revised our consent mechanisms for obtaining personal data, ensuring that individuals understand what they are providing, why and how we use it and giving clear, defined ways to consent to us processing their information. We have developed stringent processes for recording consent, making sure that we can evidence an affirmative opt-in, along with time and date records; and an easy-to-see and access way to withdraw consent at any time.
- **Direct marketing** - – We have revised the wording and processes for direct marketing, including clear opt-in mechanisms for marketing subscriptions; a clear notice and method for opting out and providing unsubscribe features on all subsequent marketing materials.
- **Data Protection Impact Assessments (DPIA)** – Where we process personal information that is considered high risk, involves large scale processing or includes special category/criminal conviction data, we have developed stringent procedures and assessment templates for carrying out impact assessments that comply fully with the UK GDPR's Article 35 requirements. We have implemented documentation processes that record each assessment, allow us to rate the risk posed by the processing activity and implement mitigating measures to reduce the risk posed to the data subject(s).

- **Processor agreements** – Where we use any third-party to process personal information on our behalf (i.e. Payroll, Recruitment, Hosting etc.), we have drafted compliant Processor Agreements and due diligence procedures for ensuring that they (as well as we), meet and understand their/our UK GDPR obligations. These measures include initial and ongoing reviews of the service provided, the necessity of the processing activity, the technical and organisational measures in place and compliance with the UK GDPR.
- **Special categories data** – **W**here we obtain and process any special category information, we do so in complete compliance with the Article 9 requirements and have high-level encryptions and protections on all such data. Special category data is only processed where necessary and is only processed where we have first identified the appropriate Article 9(2) basis or the Data Protection Bill Schedule 1 condition. Where we rely on consent for processing, this is explicit and is verified by a signature, with the right to modify or remove consent being clearly signposted.

## Information security and technical and organisational measures

NetSupport Group takes the privacy and security of individuals and their personal information very seriously and takes every reasonable measure and precaution to protect and secure the personal data that we process. We have robust information security policies and procedures in place to protect personal information from unauthorised access, alteration, disclosure or destruction. The exception to this would be where we are requested by law enforcement to provide this information.

## GDPR roles and employees

**NetSupport Group** has designated **Helen Hankinson** as our **Data Protection Officer (DPO)** and has appointed a data privacy team to continue to develop and implement our roadmap for complying with any required data protection Regulation. The team is responsible for promoting awareness of the UK GDPR across the organisation, assessing our UK GDPR readiness, identifying any gap areas and implementing the new policies, procedures and measures.

NetSupport Group understands that continuous employee awareness and understanding is vital to the continued compliance of the UK GDPR, and has involved our employees in our activities and plans. We have implemented an employee training programme specific to the needs of employee roles which forms part of our induction and annual training programme.

If you have any questions about our culture around data protection, or the UK GDPR specifically, please contact the **Data Protection team.**

**Data Protection Officer contact details:**

**Name:** Helen Hankinson
**Address:** NetSupport House,
Towngate East,
Market Deeping,
Peterborough, PE6 8NE,
United Kingdom
**Email:** dpo@netsupportsoftware.com
**Tel:** +44 (0)1778 382270