NCI Technologies Ltd.
Waterside House
Falmouth Road
Penryn
Cornwall
TR10 8BE

01326 379 497
sales@ncitech.co.uk

NCI Technologies Ltd - Data Privacy Policy

Creation Date: 20/05/2018

Last update: 24/05/2018

Revision: 1.00

Contents

NCI Technologies take your privacy seriously, and will only use personal information to administer your account and to undertake any commitments we have to our customers as part of our contracted services.

This document outlines the data we collect and how it is used.

The data we collect about you

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

We may collect, use, store and transfer different kinds of personal data about you which we have grouped together as follows:

Identity Data

Includes first name, maiden name, last name, username or similar identifier, title, job function.

Contact Data

Includes billing address, delivery address, business address, email address and telephone numbers.

Financial Data

Includes bank account details.

Transaction Data

Includes details about payments to and from you, support calls logged, service and sales requests and other details of products and services you have purchased from us.

Technical Data

If you have a support contract with NCI or other managed service we may also collect the following information: internet protocol (IP) address, operating system, hardware specifications, software installed and platform and other technology on the devices you use, system specifications, network diagrams, usernames and passwords of network devices and administration accounts (where relevant).

Profile Data

Includes your username and password to access our help desk, the vertical that your business operates in, total number of desktops and servers in your business.

Usage Data

Includes information about how you use our website.

Marketing and Communications Data

Includes your preferences in receiving marketing from us and your communication preferences.

We do not collect any Special Categories of Personal Data about you (this includes details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union

membership, information about your health and genetic and biometric data). Nor do we collect any information about criminal convictions and offences.

How is your personal data collected?

We use different methods to collect data from and about you including through:

Direct interactions.

You may give us your Identity, Contact and Financial Data by filling in forms or by corresponding with us by post, phone, email or otherwise. This includes personal data you provide when you:

- Apply for our products or services;
- Create an account on our help desk;
- Subscribe to our services or email newsletters;
- Request marketing to be sent to you;
- Enter a competition, promotion or survey;
- Provide us with some feedback.

Automated technologies or interactions.

As you interact with our website, we may automatically collect Technical Data such as ip address, browsing actions and patterns. We collect this data by using, server logs and other similar technologies.

If you have a managed support contract with us that includes monitoring of desktops and/or servers, our monitoring software will collect the following core data:

Hardware specifications, software installed, last logged on user, errors and alerts generated on servers and desktops, status of backup, status of desktop patching, status of anti-virus, online status of desktops and servers. Please note that we DO NOT collect browsing history or any information about your web usage.

In addition to this if you are subscribing to any service from us will also collect error and alerts generated by the service, such as an internet outage, firewall error alerts, failed backup, failed hardware, hardware offline alerts.

Third parties or publicly available sources.

We may receive personal data about you from various third parties as set out below:

Technical Data from the following parties:

- analytics providers, Google;
- social media providers such as twitter, facebook, instagram, linkedin;
- business contact data and business profile data from providers of marketing services.

How we use your personal data

We will only use your personal data when the law allows us to. Most commonly, we will use your personal data in the following circumstances:

Where we need to perform the contract we are about to enter into or have entered into with you. Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests. Where we need to comply with a legal or regulatory obligation.

See below to find out more about the types of lawful basis that we will rely on to process your personal data.

Generally, we do not rely on consent as a legal basis for processing your personal data other than in relation to sending direct marketing communications to you via email. You have the right to withdraw consent to marketing at any time by contacting us.

Purposes for which we will use your personal data

We have set out below in table format, a description of all the ways we plan to use your personal data, and which of the legal bases we rely on to do so. We have also identified what our legitimate interests are where appropriate.

Note that we may process your personal data for more than one lawful grounds depending on the specific purpose for which we are using your data. Please contact us if you need details about the specific legal ground we are relying on to process your personal data where more than one ground has been set out in the table below.

Purpose/Activity	**Type of Data**	**Lawful basis for processing including basic of legitimate interest**
To register you as a new customer	identity / contact	Performance of a contract with you
To process and deliver your order	identity / contact	Performance of a contract with you
Manage payments, fees and charges	financial / transactional	Necessary for our legitimate interests (to recover debts due to us)
Email you technical and security information	identity / contact / technical	Performance of a contract with you, our legitimate interest to advise you of security threats and relevant IT services to your business.
Asking you to leave a review or take a survey	identity / contact / technical / transactional	Our legitimate interests to ensure we are provide a high level of service and to change our business processes accordingly

To make suggestions and recommendations to you about goods or services that may be of interest to you	identity / contact / technical / profile	Necessary for our legitimate interests (to develop our products/services and grow and survive as a business) Frequency of sending this information will be kept to a minimum and we will offer the ability to opt out in every message.
Notifying you about changes to our terms, services or policies	contact, profile	Necessary to comply with our legal obligations
Contact you about your account	contact, financial, transactional	Necessary for our legitimate interests to recover debts due to us and pay our suppliers

Marketing

We strive to provide you with choices regarding certain personal data uses, particularly around marketing and advertising:

Promotional offers from us

We may use your Identity, Contact, and Profile Data to form a view on what we think you may want or need, or what may be of interest to you. This is how we decide which products, services and offers may be relevant for you.
Our promotion offers are sent business to business and not to individual consumers, we will always include an opt out link in the email you receive from us.
Our intention is to make any direct marketing information pertinent to the development of your business infrastructure, it's security and employee productivity and to keep you informed of new products and services as we develop them.

Third-party marketing

We will get your express opt-in consent before we share your personal data with any company outside the NCI for marketing purposes.

Opting Out

You can opt out any time by sending an email to help@ncitech.co.uk with a message to tell us you wish to opt out of our marketing.

Where you opt out of receiving these marketing messages, this will not apply to communications we send as a result of a product/service purchase, warranty registration, product/service experience or other transactions.

Change of purpose

We will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If

you wish to get an explanation as to how the processing for the new purpose is compatible with the original purpose, please contact us on 01326 379 497 or by email to help@ncitech.co.uk

If we need to use your personal data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal data without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

Disclosures of your personal data

We may have to share your personal data with the parties set out below for the purposes set out in the table above.

Third parties to whom we may choose to sell, transfer, or merge parts of our business or our assets. Alternatively, we may seek to acquire other businesses or merge with them. If a change happens to our business, then the new owners may use your personal data in the same way as set out in this privacy notice.

Other third parties with which we may share your data, include our business partners, suppliers and manufacturers. We require all third parties to respect the security of your personal data and to treat it in accordance with the law. We do not allow our third-party service providers to use your personal data for their own purposes and only permit them to process your personal data for specified purposes and in accordance with our instructions.

Third parties that we may share your personal data are:

- Internet service provides where it relates to a service you have from us or are ordering.
- NCI's Hardware and Software Suppliers and Vendors, where it relates to an order, warranty issue or service that you have or are ordering from us.
- Other NCI business partners, where it relates to a product or services you have or are ordering from us.

International transfers

When we share your personal data with our suppliers and vendors it may involve transferring your data outside the European Economic Area (**EEA**). We will only share personal data with our suppliers and vendors if absolutely necessary when it relates to a product or service you have from us or are ordering from us. Sharing of this data is infrequent and will only be done when both NCI and your business have a legitimate interest related to a product or service you are engaging with us about and when such interest is not overridden by the rights of you as an individual.

Some of our external third parties have offices based outside the European Economic Area (**EEA**) so their processing of your personal data may involve a transfer of data outside the EEA.

Whenever we transfer your personal data out of the EEA, we ensure a similar degree of protection is afforded to it by ensuring at least one of the following safeguards is implemented:

We will only transfer your personal data to countries that have been deemed to provide an adequate level of protection for personal data by the European Commission. For further details, see European Commission: Adequacy of the protection of personal data in non-EU countries.

Where we use providers based in the US, we may transfer data to them if they are part of the Privacy Shield which requires them to provide similar protection to personal data shared between the Europe and the US. For further details, see European Commission: EU-US Privacy Shield. https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-privacy-shield_en

Data security

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

Data held by NCI resides in multiple databases and storage locations, our core databases and network are protected by multi factor authentication in which a staff member is granted access only after successfully presenting 2 or more pieces of evidence (or factors) to an authentication mechanism: these factors consist of 2 or more of the following factor types: knowledge (something they and only they know), possession (something they and only they have), and inherence (something they and only they are).

NCI will be following the guidelines as defined in GDPR in the spirit in which they are written, this includes ensuring that all personal identifiable data is held securely and encrypted where applicable this includes both data held at rest and in transmission to our customers or any other 3rd party.

Access to your data

If you are a contracted customer with NCI and are currently paying for a monthly or annual support contract certain members of our staff will have remote access to your desktops, servers and network devices. The purpose of this access is to fulfil our contracted obligations to you (providing IT support and service). All access to your systems is controlled and audited and performed through our remote access system. The remote access system is only accessed by named user accounts and access logs are maintained for a period of 6 months. Data audited by this remote access system includes session events such as, connects, disconnects, transfers, NCI staff user account name, host names and ip addresses.

As part of our commitment to you NCI Technologies will never access or remove any data from your systems without your express consent. All data that NCI Technologies has access to will only be accessed to fulfil our obligations to you as an IT service provider, for example; restoration of files, checking backups or any other

IT request that we need to undertake as part of your contract or agreement with us.
Such access has been compartmentalised and NCI staff members only have access to certain data if they require it as part of their job function.

Data retention

We will only retain your personal data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

Your legal rights

Under certain circumstances, you have rights under data protection laws in relation to your personal data. These include: Request access to your personal data, Request correction of your personal data, Request erasure of your personal data, Object to processing of your personal data, Request restriction of processing your personal data, Request transfer of your personal data or Right to withdraw consent.

If you wish to exercise any of the rights set out above, you can do so by contacting us on 01326 379 497 or by sending an email to help@ncitech.co.uk

No fee usually required

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we may refuse to comply with your request in these circumstances.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

Time limit to respond

We try to respond to all legitimate requests within one month. Occasionally it may take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

Glossary

LAWFUL BASIS

Legitimate Interest means the interest of our business in conducting and managing our business to enable us to give you the best service/product and the best and most secure experience. We make sure we consider and balance any potential impact on you (both positive and negative) and your rights before we process your personal data for our legitimate interests. We do not use your personal data for activities where our interests are overridden by the impact on you (unless we have your consent or are otherwise required or permitted to by law). You can obtain further information about how we assess our legitimate interests against any potential impact on you in respect of specific activities by contacting us.

Performance of a Contract means processing your data where it is necessary for the performance of a contract or service to which you are a party or to take steps at your request before entering into such a contract.

Comply with a legal or regulatory obligation means processing your personal data where it is necessary for compliance with a legal or regulatory obligation that we are subject to.

THIRD PARTIES

External Third Parties

Service providers acting as processors who provide IT and system administration services. Professional advisers acting as processors or joint controllers including lawyers, bankers, auditors and insurers who provide consultancy, banking, legal, insurance and accounting services.

HM Revenue & Customs, regulators and other authorities who require reporting of processing activities in certain circumstances.

YOUR LEGAL RIGHTS

You have the right to:

Request access to your personal data (commonly known as a "data subject access request"). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.

Request correction of the personal data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.

Request erasure of your personal data. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your personal data to comply with local law. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.

Object to processing of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your personal data for direct marketing purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms.

Request restriction of processing of your personal data. This enables you to ask us to suspend the processing of your personal data in the following scenarios: (a) if you want us to establish the data's accuracy; (b) where our use of the data is unlawful but you do not want us to erase it; (c) where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims; or (d) you have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.

Request the transfer of your personal data to you or to a third party. We will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.

Withdraw consent at any time where we are relying on consent to process your personal data. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent.

Contact Details

NCI Technologies Ltd
Waterside House
Falmouth Road
Penryn
Cornwall
TR10 8BE

Tel: 01326 379 497

Email: help@ncitech.co.uk