“Cerberus” Privacy Overview

On May 25, 2018, the European Union’s General Data Protection Regulation (GDPR) took effect. GDPR regulates the governance of personal data for European Union (EU) citizens with an emphasis on data security and privacy. The GDPR does not only apply to companies that operate in the EU. This regulation will also impact companies operating outside of the EU if they have any EU customers or personal data of anyone in the EU.

Cerberus and www.trustcerberus.com are trading names of Netcom Data Services Limited. Netcom has made information security and data privacy principles the foundation of everything we do, and we recognise the importance of passing regulations to advance information security and data privacy for citizens of the EU. **We take special pride in our role in helping Clients get ready for GDPR and demonstrating how our products help to provide a more secure environment for our customers.** We are firmly committed to GDPR readiness.

How we handle our customers privacy

This document is an overview of how we handle privacy and includes:

- The types of information we collect
- How we collect and use it
- Who we might share it with
- The steps we’ll take to make sure it stays private and secure
- Your rights to your information

More information

For more details about anything covered in this overview, please call us a call on 0800 256 1692 or email team@trustvcerberus.com

Who we are

When we say ‘we’, ‘us’ or ‘our’, we mean Netcom Data Services Ltd or Netcom Technologies Ltd who is the ‘data processor’ for the information in this overview. When we say ‘you’ or ‘customer’ we mean the company or client we are providing services to, which may include employees of the company we are providing services and information provided by the customer who, being a company would have a person responsible as the ‘Data Processor’ who is responsible for deciding how we can use the information we hold. When we say ‘customer data’ this means files and documents owned by the customer.

The information we collect

We collect information from different places including:

- Directly from our customers and our customers employees
- From our customers IT and business systems and computers (from our Customers IT Infrastructure and business Systems)
- From publicly available sources
- When we generate it ourselves
- From other organisations

We'll only collect information in line with relevant regulations and law and this may relate to any of our products or services our customers enquire about, are able to receive, currently hold or have held in the past.

Our customers data processor is responsible for making sure our customers give us accurate and up to date information.

The types of data we process

Depending on the Offering chosen by the customer, we will process on behalf of the customer the following personal data:

- First Name
- Last Name
- Mailing Address
- Email Address
- Business Phone
- Mobile Phone
- Home or personal phone
- Computer Name
- Computer IP address
- Computer MAC address
- Computer access password

In addition, we may process, under the terms as detailed in our general terms and conditions, personal data which the customer elects to host with or upload to us in connection with the our provision of services to our customers. Our systems hold logs of customer data and use, we keep these logs for a reasonable amount of time to help troubleshooting issues. These logs are not passed on or sold.

How we'll use the information

We'll use it to provide any products and services our customer has requested and other purposes including:

- To confirm your identity and address
- To understand how our customers use our services

- To carry out our customers instructions and deliver services
- To improve our products and services
- To offer other services which we believe may benefit our customers unless you ask us not to.

We'll only use our customers information where we're allowed to by law e.g. carrying out an agreement and providing services for our customers, fulfilling a legal obligation, because we have a legitimate business interest or where our customers agree to it.

What we do to ensure our customers information is safe

Any suppliers who we share personally identifiable information with have given their assurance of their commitment to the GDPR and the requirements contained therein.

When choosing new suppliers we look for suppliers who have achieved ISO27001, Cyber Essentials, Privacy Shield or another related certification or that can demonstrate competence and adherence to good privacy and security standards.

As a Government accredited certification body for IASME/Cyber Essentials, we undergo stringent annual inspections. This is not only part of our commitment to attaining the highest levels of Cyber Security for our clients and the information we hold, it is also needed to allow us to assess other businesses regarding their levels of cyber security, GDPR readiness and to issue IASME certificates to show our clients have attained the Government approved level of security. We have achieved IASME GOLD status showing that procedures, processes and systems we have in place not only meet the UK Government endorsed IASME/Cyber Essential Standards but surpass it to GOLD standard. Our certification can be found here.

A few of the physical measures we take are:

- All devices we use to store information are encrypted,
- Our business systems are both encrypted and protected by two (and three) factor authentication meaning that we need to pass at least 2x security challenges to gain access to business systems. In addition to that, we use systems which change the login password every 30 seconds to further reduce the risk of intrusion
- Our engineers use password management systems which mean that they are given admin passwords when needed and that password is changed shortly after
- We will never send a password over unencrypted email or plain text and use encryption and other means to ensure that passwords remain a secret.
- As well as using firewalls and regularly patching and applying updates, we incorporate intrusion detection and system vulnerability systems and regularly perform penetration testing of our own security.
- Our staff have certified training in relation to Cyber Security.

- That's not to mention our perimeter security and building two factor authentication, razor wire and guard dogs, okay we don't have guard dogs.

The above lists 7 of the 165 methods incorporated to fulfill our IASME/Cyber Essentials standards. We're not giving anything away as these are publicly available. There are many other ways that we protect ourselves and our client's information which are best kept to ourselves to keep our security, well, secure.

Who we share your information with

We may share our customers information with other companies we work in partnership with. These include carefully selected suppliers who provide our warranty support, updating, business systems and storage systems. Our customers can request a list of the suppliers we use to process personal data. We also use 3rd party suppliers to provide platforms to store and manage our customers data. For example, we use Microsoft's Azure cloud systems and the Office365 platform to store our customer information and data, as a supplier we have ensured that the customer data stored with Microsoft is encrypted, stored in the EU and not stored for longer that is needed. Our customer data belongs to our customers and as such we don't store it for anything other than providing specific storage services (such as backup). We don't share our customers information with any parties other than for the provision of services to the customer or to improve our products or services. We apply the same methodology for all our suppliers.

How long we'll keep information

We'll keep our customers information and customers data for as long as our customer has a relationship with us. After it ends we'll keep it for a pre-defined period thereafter and where we may need it for our legitimate purposes e.g. to help us respond to queries or complaints, or for other reasons e.g. fighting fraud, crime, and responding to requests from regulators.

The types of data we keep and how long we keep it:

Data Type	Summary of what this may contain	Retention period	Reason for retention
Customer Information	Customers business address, service users details, usernames, email addresses, passwords, IP addresses, system details, contact details including (where needed for service) home address and	36 months	Sometimes customers ask for information after moving to another provider. Many customers come back to Netcom when the contract with a replacement provided ends, keeping the information on file helps the migration process. We'll also use the information to inform around new products and

	personal contact details.		services which may help the customer.
Customer Data	Customers backups, copies of documents	We retain backups for the duration of providing the backup service. We do not retain customers documents for any longer than is needed to complete the work being performed.	We keep backups as part of the backup service we provide. We keep documents for as short time as possible whilst working on a job which requires us to use the documents and only with the permission of the sender.

Transferring your information overseas

Your information may be transferred and stored in countries outside the European Economic Area, including some that may not have laws that provide the same level of protection for personal information. When we do this, we seek confirmation from the supplier that they have the appropriate levels of protection. This can include membership of EU-US Privacy Shield and other international data privacy arrangements.

Your rights

Our customers have rights relating to their information e.g. to see what we hold, to ask us to share it with another party, ask us to update incorrect or incomplete details, to object to or restrict processing of it please email dpo@netcomtech.co.uk or contact the person responsible for data as detailed at the bottom of this page.

You have the right to lodge a complaint with the Information Commissioners Office (ICO) if you believe your data has been processed in a way that does not comply with the GDPR. You can do so by calling the ICO helpline on **0303 123 1113 or via their website.**

Our contact information

The person responsible for data protection is:

Mark Kindred

Cerberus

SilverStamp House

Club Mill Road

Sheffield

S6 2FH

Email: dpo@netcomtech.co.uk

Tel: 0800 256 1692