Data Retention Policy

1. Introduction

This Policy sets out the obligations of CenCom Solutions Ltd., a company registered in England and Wales under number 04723715, whose registered office is at The Coppice, Petteridge Lane, Matfield. Kent, TN12 7LP ("the Company") regarding retention of personal data collected, held, and processed by the Company in accordance with EU Regulation 2016/679 General Data Protection Regulation ("GDPR").

The GDPR defines "personal data" as any information relating to an identified or identifiable natural person (a "data subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

The GDPR also addresses "special category" personal data (also known as "sensitive" personal data). Such data includes, but is not necessarily limited to, data concerning the data subject's race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation.

Under the GDPR, personal data shall be kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. In certain cases, personal data may be stored for longer periods where that data is to be processed for archiving purposes that are in the public interest, for scientific or historical research, or for statistical purposes (subject to the implementation of the appropriate technical and organisational measures required by the GDPR to protect that data).

In addition, the GDPR includes the right to erasure or "the right to be forgotten". Data subjects have the right to have their personal data erased (and to prevent the processing of that personal data) in the following circumstances:

a) Where the personal data is no longer required for the purpose for which it was originally collected or processed (see above);

b) When the data subject withdraws their consent;

c) When the data subject objects to the processing of their personal data and the Company has no overriding legitimate interest;

d) When the personal data is processed unlawfully (i.e. in breach of the GDPR);

e) When the personal data has to be erased to comply with a legal obligation; or

f) Where the personal data is processed for the provision of information society services to a child.

This Policy sets out the type(s) of personal data held by the Company for the purposes of providing technical management and support to individuals and businesses, the period(s) for which that personal data is to be retained, the criteria for establishing and reviewing such period(s), and when and how it is to be deleted or otherwise disposed of.

For further information on other aspects of data protection and compliance with the GDPR, please refer to the Company's Data Protection Policy.

2. Aims and Objectives

2.1 The primary aim of this Policy is to set out limits for the retention of personal data and to ensure that those limits, as well as further data subject rights to erasure, are complied with. By extension, this Policy aims to ensure that the Company complies fully with its obligations and the rights of data subjects under the GDPR.

2.2 In addition to safeguarding the rights of data subjects under the GDPR, by ensuring that excessive amounts of data are not retained by the Company, this Policy also aims to improve the speed and efficiency of managing data.

3. Scope

3.1 This Policy applies to all personal data held by the Company and by third-party data processors processing personal data on the Company's behalf.

3.2 Personal data, as held by the Company is stored in the following ways and in the following locations:

a) The Company's servers, located in The Coppice, Matfield and Custodian Data Centre Maidstone;

b) Third-party servers, operated by Microsoft and located in The UK and within the EU;

c) Computers permanently located in the Company's premises at The Coppice, Matfield;

d) Laptop computers and other mobile devices provided by the Company to its employees;

e) Computers and mobile devices owned by employees, agents, and sub-contractors used in accordance with the Company's Bring Your Own Device ("BYOD") Policy**;**

f) Physical records stored in The Coppice, Matfield;

g) Backup Locations stored Operated by SolarWinds within the EU.

4. Data Subject Rights and Data Integrity

All personal data held by the Company is held in accordance with the requirements of the GDPR and data subjects' rights thereunder, as set out in the Company's Data Protection Policy.

4.1 Data subjects are kept fully informed of their rights, of what personal data the Company holds about them, how that personal data is used as set out the Company's Data Protection Policy, and how long the Company will hold that personal data (or, if no fixed retention period can be determined, the criteria by which the retention of the data will be determined).

4.2 Data subjects are given control over their personal data held by the Company including the right to have incorrect data rectified, the right to request that their personal data be deleted or otherwise disposed of (notwithstanding the retention periods otherwise set by this Data Retention Policy), the right to restrict the Company's use of their personal data, the right to data portability, and further rights relating to automated decision-making and profiling, as set out in Parts 14 to 20 of the Company's Data Protection Policy**.**

5. Technical and Organisational Data Security Measures

5.1 The following technical measures are in place within the Company to protect the security of personal data. Please refer to Parts 22 to 26 of the Company's Data Protection Policy for further details:

a) All emails containing personal data must be encrypted;

b) All emails containing personal data must be marked "confidential";

c) Personal data may only be transmitted over secure networks;

d) Personal data may not be transmitted over a wireless network if there is a reasonable wired alternative;

e) Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself and associated temporary files should be deleted;

f) Where personal data is to be sent by facsimile transmission the recipient should be informed in advance and should be waiting to receive it;

g) Where personal data is to be transferred in hardcopy form, it should be passed directly to the recipient**;**

h) All personal data transferred physically should be transferred in a suitable container marked “confidential”;

i) No personal data may be shared informally and if access is required to any personal data, such access should be formally requested from the data protection officer.

j) All hardcopies of personal data, along with any electronic copies stored on physical media should be stored securely;

k) No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, without authorisation;

l) Personal data must be handled with care at all times and should not be left unattended or on view;

m) Computers used to view personal data must always be locked before being left unattended;

n) No personal data should be stored on any mobile device, whether such device belongs to the Company or otherwise without the formal written approval of the data protection officer and then strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is necessary;

o) No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the Company’s Data Protection Policy and the GDPR;

p) All personal data stored electronically should be backed up Daily with backups stored offsite. All backups should be encrypted;

q) All electronic copies of personal data should be stored securely using passwords and encryption;

r) All passwords used to protect personal data should be changed regularly and must be secure;

s) Under no circumstances should any passwords be written down or shared. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;

t) All software should be kept up-to-date. Security-related updates should be installed not more than a week after becoming available;

u) No software may be installed on any Company-owned computer or device without approval; and

v) Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of the data protection officer to ensure that the appropriate consent

is obtained and that no data subjects have opted out, whether directly or via a third-party service such as the TPS.

5.2 The following organisational measures are in place within the Company to protect the security of personal data. Please refer to Part 27 of the Company's Data Protection Policy for further details:

a) All employees and other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the GDPR and under the Company's Data Protection Policy;

b) Only employees and other parties working on behalf of the Company that need access to, and use of, personal data in order to perform their work shall have access to personal data held by the Company;

c) All employees and other parties working on behalf of the Company handling personal data will be appropriately trained to do so;

d) All employees and other parties working on behalf of the Company handling personal data will be appropriately supervised;

e) All employees and other parties working on behalf of the Company handling personal data should exercise care and caution when discussing any work relating to personal data at all times;

f) Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;

g) The performance of those employees and other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed;

h) All employees and other parties working on behalf of the Company handling personal data will be bound by contract to comply with the GDPR and the Company's Data Protection Policy;

i) All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all relevant employees are held to the same conditions as those relevant employees of the Company arising out of the GDPR and the Company's Data Protection Policy;

j) Where any agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under the GDPR and/or the Company's Data Protection Policy, that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

6. Data Disposal

Upon the expiry of the data retention periods set out below in Part 7 of this Policy, or when a data subject exercises their right to have their personal data erased, personal data shall be deleted, destroyed, or otherwise disposed of as follows:

6.1 Personal data stored electronically shall be deleted;

6.2 Personal data stored in hardcopy form shall be shredded and recycled;

7. Data Retention

7.1 As stated above, and as required by law, the Company shall not retain any personal data for any longer than is necessary in light of the purpose(s) for which that data is

collected, held, and processed.

7.2 Different types of personal data, used for different purposes, will necessarily be retained for different periods and its retention periodically reviewed, as set out below.

7.3 When establishing and/or reviewing retention periods, the following shall be taken into account:

a) The objectives and requirements of the Company;

b) The type of personal data in question;

c) The purpose(s) for which the data in question is collected, held, and processed;

d) The Company's legal basis for collecting, holding, and processing that data;

e) The category or categories of data subject to whom the data relates;

7.4 If a precise retention period cannot be fixed for a particular type of data, criteria shall be established by which the retention of the data will be determined, thereby ensuring that the data in question, and the retention of that data, can be regularly reviewed against those criteria.

7.5 Notwithstanding the following defined retention periods, certain personal data may be deleted or otherwise disposed of prior to the expiry of its defined retention period where a decision is made within the Company to do so (whether in response to a request by a data subject or otherwise).

7.6 In limited circumstances, it may also be necessary to retain personal data for longer periods where such retention is for archiving purposes that are in the public interest, for scientific or historical research purposes, or for statistical purposes. All such retention will be subject to the implementation of appropriate technical and organisational measures to protect the rights and freedoms of data subjects, as required by the GDPR.

Data Ref.	Type of Data	Purpose of Data	Lawful Purpose	Review Period	Retention Period or Criteria	Comments
OLK01	Subject Name, email, phone numbers and postal address	Identify Correspondent, facilitate communication to reply to and initiate related to services agreed in service agreement	Contract \ Legitimate Interest	Annual	Up to 12 months after the contact is no longer corresponded with	Individual users are responsible for ensuring their contacts are clear of old contacts annually, new contacts are added automatically but cannot be removed the same way however they are marked for removal if the contact is no longer under contract.
DYN01	Subject Name, email, phone numbers and postal address	Identify Correspondent, facilitate communication to reply to and initiate related to services agreed in service agreement	Contract \ Legitimate Interest	Annual	Up to 12 months after the contact is no longer corresponded with	Clients under contract are removed when their contract is no longer in force, supplier and 3rd party are reviewed annually for removal.
DYN04	Subject Name, email, Logon Name	Provide knowledge and information about their contracted services and safety or user information about their systems	Contract	Monthly	30 days after contract is no longer in force.	We remove individual information when the company no longer has a contract. This is done at the next billing cycle.
QB01	Subject Name, email, phone numbers and postal address	Supply and storage of invoices for services agreed in the service agreement	Contract / Legal requirement	Monthly	7 years	We are required to keep invoice records going back 7 years but review the records which are live each month when invoices are raised for services.
SP01	Subject Name and email address stored in documents	Schedules of services and definitions in service and agreements and stored correspondence	Contract / Legitimate interest	Annual	Up to 12 months after a contract has finished	We review and remove old data from SharePoint annually, this data is removed during a client sign off process, This is in case there are documents relating to warranty for hardware or other areas we may hold.
OLK02	Subject Name and email address stored in emails	Storage for reference of communication	Contract / Legitimate interest	Annual	2 years after which or if legal action is underway until the resolution of that action	All emails are deleted once they become two years old, unless a legal hold is placed on the mails because they are required to protect the interest of CenCom or others.
DYN05	Supplier Subject Name and email address	Communication with 3rd parties related to services they provide to CenCom clients.	Legitimate interest	Annual	Up to one year after a client using the supplier has no need for them	Every year the 3rd party contacts for clients are reviewed and those no longer required removed.
DYN06	Supplier Subject	Communication with	Contract /	Annual	Until goods and	Each contact is reviewed for the services and

	Name and email address	parties related to services they provide to CenCom itself.	Legitimate interest		services provided to CenCom have completed any warrantee or other service component	equipment provided and only removed when there is no chance we will need to exercise any rights through that supplier.
DYN02	Subject Name and email address stored in emails	Storage for reference of communication	Contract / Legitimate interest	Monthly	12 Months after contact with client has ceased	We retain information from clients correspondence for enough time to ensure we can provide context to any actions we have taken during the service such as change requests.
DYN03	Subject Name and Asset ID	Subject Name and Asset ID	Contract / Legitimate interest	Monthly	12 Months after contact with client has ceased	We retain information from clients correspondence for enough time to ensure we can provide context to any actions we have taken during the service such as change requests.
SOW01	Subject Name and Logon ID	Monitor computers during provision of service	Contract	Monthly	30 days after service contract is ceased	This is a service we pay for so must be ceased when no longer provided. Information should be provided to the client if requested before removal
SOW02	IP Address and MAC Address	Monitor computers during provision of service	Contract	Monthly	30 days after service contract is ceased	This is a service we pay for so must be ceased when no longer provided. Information should be provided to the client if requested before removal
DYN03	IP Address	Identify Location of specific hardware	Contract	Monthly	12 Months after contact with client has ceased	We retain information from clients hardware for enough time to ensure we can provide context to any actions we have taken during the service such as change requests.
RDM01	IP Address, Domain Name	Facilitate remote connection to servers and services.	Contract	Monthly	30 days after contract is ceased	This is for the provision of service and once the contact is ceased these records are deleted as part of the client removal process
FAH01	Name, email, Postal Address	Manage Domain Names their and contacts.	Contract / Legitimate Interest	Annually	Immediately on request	These are part of the domain registration and required to fulfil the service, until the client has moved their domain to another provider these reqords are required
TRC01	Name, email, Postal Address	Manage Certificates and their contacts	Contract	Annually	On Expiration	These form part of the security certificates we supply, the records are removed when the certificate expires and will not be re-added unless a new certificate is purchased.
ESX01	Name and Mobile Phone Number	Notification by text to clients of service issues or	Legitimate interest	Monthly	None	The information is maintained as part of the billing information of who text messages are sent to and

		in response to open service requests.				cannot be removed.
SOW03	Name, Phone, Last logon time, last password change	Output of Active Directory to provide diagnostic information for reporting.	Contract	Monthly	30 days	This data is gathered and renewed daily and kept for 30 days and automatically overwritten
SOW04	Name, IP Address, Software Version, Computer identification and specification	Output of Hardware monitoring to provide diagnostic information and reporting.	Contract	Monthly	30days	This data is gathered and renewed daily and kept for 30 days and automatically overwritten
SOW05	Name, IP Address, Websites Visited, Bandwidth Used	Output of web filtering and protection to provide diagnostic information and reporting.	Contract	Monthly	30days	This data is gathered and renewed daily and kept for 30 days and automatically overwritten

8. Roles and Responsibilities

8.1 The Company's Data Protection Officer is, Cenydd Milne.

8.2 The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the Company's other Data Protection-related policies (including, but not limited to, its Data Protection Policy), and with the GDPR and other applicable data protection legislation.

8.3 The Data Protection Officer shall be directly responsible for ensuring compliance with the above data retention periods throughout the Company.

8.4 Any questions regarding this Policy, the retention of personal data, or any other aspect of GDPR compliance should be referred to the Data Protection Officer.

9. Implementation of Policy

This Policy shall be deemed effective as of 01/04/2018. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy has been approved and authorised by:

Name:	Cenydd Milne
Position:	Technical Director
Date:	01/04/2018
Due for Review by:	01/04/2019
Signature:	