PRIVACY & GDPR POLICY

VIRIDIAN PRIVACY POLICY

1. INTRODUCTION

1.1.
We are committed to safeguarding the privacy of our VIRIDIAN service users.

1.2.
This policy applies where we are acting as a data controller with respect to the personal data of VIRIDIAN service users; in other words, where we determine the purposes and means of the processing of that personal data.

1.3.
In this policy, "we", "us" and "our" refer to ICTS UK. For more information about us, see Section 12.

2. HOW WE USE PERSONAL DATA

2.1.
In this Section 2 we have set out:
a) the general categories of personal data that we may process;
b) in the case of personal data that we did not obtain directly from you, the source and specific categories of that data;
c) the purposes for which we may process personal data
d) the legal bases of the processing.

2.2.
We may process service users account data ("account data").
The account data may include your name and email address. The source of the account data is you or your employer.

The account data may be processed for the purposes of operating our VIRIDIAN website, providing our VIRIDIAN services, ensuring the security of our VIRIDIAN website and VIRIDIAN services and communicating with service users. The legal basis for this processing is our legitimate interests, namely the proper administration of our VIRIDIAN website and VIRIDIAN service.

PRIVACY & GDPR POLICY

2.3.
We may process information of vendors or other staff arriving to the clients site which may include the following;

a) Full name
b) Badge details
c) ID number, or copy of the ID
d) Phone number or email
e) Purpose of your visit to the site
f) Any incident related information

2.4.
Please do not supply any other person's personal data to us, unless we prompt you to do so.

3. PROVIDING YOUR PERSONAL DATA TO OTHERS

3.1.
We may disclose personal data to any member of our group of companies (this means our subsidiaries, our ultimate holding company and partners) in so far as reasonably necessary for the purposes of auditing VIRIDIAN activities and ensuring that the appropriate level of service is provided to clients. The legal basis for this is our legitimate interests, namely ensuring that the correct level of service is being provided to clients.

3.2.
In addition to the specific disclosures of personal data set out in this Section 3, we may disclose personal data where such disclosure is necessary for compliance with a legal obligation to which we are subject, or in order to protect your vital interests or the vital interests of another natural person. We may also disclose personal data where such disclosure is necessary for the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of- court procedure.

PRIVACY & GDPR POLICY

4. INTERNATIONAL TRANSFERS OF YOUR PERSONAL DATA

4.1.
In this Section 4, we provide information about the circumstances in which your personal data may be transferred to countries outside the European Economic Area (EEA).

4.2.
Viridian is hosted on AWS cloud computing platform. While we limit the hosting of VIRIDIAN related data, including users personal data, to locations within the EEA, there may be instances when personal data is transferred outside of the EEA in order to maintain the availability of the VIRIDIAN service, such as in the event of a data centre or network outage or technical support. The AWS platform's technical and organizational measures as well as their compliance and trust documentation can be found at:

https://docs.aws.amazon.com/whitepapers/latest/aws-risk-and-compliance/welcome.html

5. RETAINING AND DELETING PERSONAL DATA

5.1.
This Section 5 sets out our data retention policies and procedure, which are designed to help ensure that we comply with our legal obligations in relation to the retention and deletion of personal data.

5.2.
Personal data that we process for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

5.3.
We will retain your personal data as follows:

Personal data type	Max retention period	Action post retention
Full name	Up to 6-12 months	Deleted

ID number (Payroll)	Up to 6-12 months	Deleted
Badge details	Up to 6-12 months	Deleted
Media (photo / video)	Up to 6-12 months	Deleted
GPS data	Up to 5 years	Deleted
Training data	Up to 5 years	Deleted
Incident Reports	Up to 5 years	Anonymized
Various activity reports	Up to 5 years	Anonymized

5.4.

Notwithstanding the other provisions of this Section 5, we may retain your personal data where such retention is necessary for compliance with a legal obligation to which we are subject, or in order to protect your vital interests or the vital interests of another natural person.

PRIVACY & GDPR POLICY

6. AMENDMENTS

6.1.
We may update this policy from time to time by publishing a new version on our website.

6.2.
We may notify you of significant changes to this policy by email.

7. SUBJECT RIGHTS

7.1.
In this Section 7, we have summarized the rights that you have under data protection law. Some of the rights are complex, and not all of the details have been included in our summaries. Accordingly, a subject should read the relevant laws and guidance from the regulatory authorities for a full explanation of these rights.

7.2.
Your principal rights under data protection law are:
(a) the right to access;
(b) the right to rectification;
(c) the right to erasure;
(d) the right to restrict processing;
(e) the right to object to processing;
(f) the right to data portability;
(g) the right to complain to a supervisory authority; and
(h) the right to withdraw consent.

7.3.
You have the right to confirmation as to whether or not we process your personal data and, where we do, access to the personal data, together with certain additional information. That additional information includes details of the purposes of the processing, the categories of personal data concerned and the recipients of the personal data. Providing the rights and freedoms of others are not affected, we will supply to you a copy of your personal data. The first copy will be provided free of charge, but additional copies may be subject to a reasonable fee.

PRIVACY & GDPR POLICY

7.4.
You have the right to have any inaccurate personal data about you rectified and, taking into account the purposes of the processing, to have any incomplete personal data about you completed.

7.5.
In some circumstances you have the right to the erasure of your personal data without undue delay.

Those circumstances include: the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; you withdraw consent to consent-based processing; you object to the processing under certain rules of applicable data protection law; the processing is for direct marketing purposes; and the personal data have been unlawfully processed. However, there are exclusions of the right to erasure. The general exclusions include where processing is necessary: for exercising the right of freedom of expression and information; for compliance with a legal obligation; or for the establishment, exercise or defence of legal claims.

7.6.
In some circumstances you have the right to restrict the processing of your personal data. Those circumstances are:

you contest the accuracy of the personal data; processing is unlawful but you oppose erasure; we no longer need the personal data for the purposes of our processing, but you require personal data for the establishment, exercise or defence of legal claims; and you have objected to processing, pending the verification of that objection. Where processing has been restricted on this basis, we may continue to store your personal data. However, we will only otherwise process it: with your consent; for the establishment, exercise or defence of legal claims; for the protection of the rights of another natural or legal person; or for reasons of important public interest.

7.7.
You have the right to object to our processing of your personal data on grounds relating to your particular situation, but only to the extent that the legal basis for the processing is that the processing is necessary for: the performance of a task carried out in the public interest or in the exercise of any official authority vested in us; or the purposes of the legitimate interests pursued by us or by a third party. If you make such an objection, we will cease to process the personal

information unless we can demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms, or the processing is for the establishment, exercise or defence of legal claims.

7.8.
You have the right to object to our processing of your personal data for scientific or historical research purposes or statistical purposes on grounds relating to your particular situation, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

7.9.
To the extent that the legal basis for our processing of your personal data is: (a) consent; or (b) that the processing is necessary for the performance of a contract to which you are party or in order to take steps at your request prior to entering into a contract, and such processing is carried out by automated means, you have the right to receive your personal data from us in a structured, commonly used and machine-readable format. However, this right does not apply where it would adversely affect the rights and freedoms of others.

7.10.
If you consider that our processing of your personal information infringes data protection laws, you have a legal right to lodge a complaint with a supervisory authority responsible for data protection. You may do so in the EU member state of your habitual residence, your place of work or the place of the alleged infringement.

7.11.
To the extent that the legal basis for our processing of your personal information is consent, you have the right to withdraw that consent at any time. Withdrawal will not affect the lawfulness of processing before the withdrawal.

7.12.
You may exercise any of your rights in relation to your personal data by written notice to us.

PRIVACY & GDPR POLICY

VIRIDIAN GDPR STATEMENT

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a privacy and data protection regulation in the European Union (EU) enforceable from the 25th of May 2018. GDPR imposes new obligations on organisations that control or process relevant personal data and introduces new rights and protections for EU data subjects.

This document is part of the Data Protection Impact Assessment (DPIA) evaluating the use of Viridian. The DPIA is an analysis of expected processing activities related to Viridian and covers details of the processing activity itself and an assessment of the risks associated with the processing activities including any measures that need to be taken to mitigate those risks. It also contains the decision on whether to initiate a prior consultation with the relevant supervisory authority. (see DPIA separately).

BACKGROUND, CONTEXT AND SCOPE

Viridian has been developed by a group of programmers and analysts with a wide experience in Data Centre security. The core of the system is a software that allows security providers and their staff to monitor and manage their activities to better comply with their SOW and contractual obligations. Also, a number of other systems and solutions will be integrated to extend the scope of Viridian.

PURPOSE OF SYSTEM

Viridian is the new data centre software solution for security and operations.
Designed and developed by ICTS, based on the vast experience with the variety types of data centres, we understand our partners needs and challenges and found creative solutions to mitigate the risks for them and their clients.

Viridian improves efficiencies, captures, and digitalizes the most critical aspects of the statement of work, prioritizes and ensures maximum compliance whilst reducing human error and increasing resilience.

Designed by the highest standard of security ensuring that all our data and our client's data is kept safely and securely.

PRIVACY & GDPR POLICY

SYSTEM DESCRIPTION

Viridian is a platform, designed, developed, and managed by ICTS Europe, provided through a web interface, that offers operational functionalities.

Users access the platform, by browsers for PC's or Apps for mobile.

Administrators, that may have different scopes of activity, for instance company groups, single companies, or locations, can:

1. Create, set up and configure contracts,
2. Create users and site accounts and update their data, if necessary
3. Create tasks and templates,
4. Affiliate activities to users, sites and events,
5. Send Notifications and reminders via e-mail or SMS,
6. Send or receive lists of enrolled users via e-mail or SMS,
7. Check data of the local users that are assigned to the country / contract / site they manage:

- the data of users or sites
- activity data
- various reports

Each administrator can see only the information related to the users that are assigned to him, based on his role and the scope of his activity (Country, contract, site).
All Viridian services and products are hosted on AWS cloud.

DATA SUBJECTS

1. The data subjects are (end users):
2. **Users**: the people that use the system on site via app or desktop.
3. **Managers**: the people that create template reports and site or personnel tasks.
4. **Administrators**: the people that set up, configure and manage users' data, site data, create tasks, generate reports and create templates.

PRIVACY & GDPR POLICY

TYPES OF PERSONALLY IDENTIFIABLE INFORMATION COLLECTED / PROCESSED

Viridian has the potential to collect the following PII data:

1. Full Name
2. Payroll number
3. Company
4. Workplace
5. Company role
6. E-Mail
7. Phone number
8. Username
9. External user ID (for integration with other systems)

SPECIAL CATEGORIES OF DATA

Viridian does not collect or process any special categories of data.

SYSTEM DESCRIPTION / DATA FLOWS

PROCESSING OPERATIONS

This section of the DPIA gives a description of the Viridian system focussing on the flow of Personally Identifiable Data within the system.

Viridian Website

As described, Viridian is a web application. All the pages of Viridian can be reached only via a browser.

REGISTRATION

PII information can be submitted by Administrators in two ways:
Compiling the fields of a form on Viridian or user details.

a) Administrators must log on the system before performing these operations.
b) User details are saved to the Viridian database.
c) For the mobile app, the user will approximate his badge to the back of the phone, allowing him to log in. For PC's, users will receive their own credentials via a password protected email.

PRIVACY & GDPR POLICY

LOG ON

a) Users submit username and password on app or Desktop, or for the mobile app, the user will approximate his badge to the back of the phone, allowing him to log in.

b) When a PC user authenticates into the platform for the first time, he/she can be forced to change his password. This is regulated by a setting in the user's record, that can be set by an administrator allowed to change the user's data, usually his responsible or the company administrator.

c) The log on procedure is the same for security officers, managers, and administrators.

VIRIDIAN REPORTS

a) Authenticated users may produce a variety of reports, some of which may contain PII information of staff or clients personnel. All reports are displayed in a tokenized web page.

b) Reports can be exported from the web page in PDF format.

SCOPE

The permissions allow access according to the users hierarchy within an organization.
For instance, a company administrator can see all the data related to the company he manages. The same for entities (groups or companies) and locations.

End users see just their personal data and operational reports.

ASSETS INCLUDING PROCESSORS AND SUB-PROCESSORS

This section of the DPIA contains a list of the assets through which personal data processing takes place, both internal and external to Viridian.

(a) **ICTS UK**, South Block, Entrance D, Tavistock House, Tavistock Square, London, WC1H 9LG. UK.

(b) **Viridian** – South Block, Entrance D, Tavistock House, Tavistock Square, London, WC1H 9LG. UK.

Viridian has developed all the code, then develops all the new features, provides system administration and customer support of the cloud based Viridian system.

(c) **AWS** - EU West 2 LDN.

Viridian is hosted on AWS cloud computing platform. The AWS platform's technical and organisational measures as well as their compliance and trust documentation can be found at: https://docs.aws.amazon.com/whitepapers/latest/aws-risk-and- compliance/welcome.html

PRIVACY & GDPR POLICY

PERSONAL DATA PROCESSED

This section describes at a high level the types of personally identifiable information that may be processed through the Viridian.

- Full Name
- Payroll number
- Company
- Workplace
- Company role
- E-Mail
- Phone number
- Date and place of Birth
- Username
- External user ID (for integration with other systems)

These data are exclusively stored for the following purposes.

- Log in users to the system
- Complete security and maintenance activities,
- Generate reports and data,
- Provide an audit trail,
- Provide KPI's,
- Manage which administrator is in charge of administering the activities of each user and site,
- Provide managers to create and update information and load documents and reports.

NECESSITY AND PROPORTIONALITY

NECESSITY

Viridian manages the activities of its users, its clients and site related activities that are registered in the system.

Viridian believes that its clients have a legitimate interest in processing personally identifiable information as part of the management of the training and activities.

PRIVACY & GDPR POLICY

Under GDPR, using a legitimate interest as a legal basis for processing can only be done so if the reason for doing so does not outweigh the rights and freedoms of the data subjects. To assess whether this is the case or not, we must look at three requirements:

- Is there a need?
- Is it warranted?
- Is it fair and lawful?

Viridian assesses that each of these requirements are met by clients of Viridian based on the following rationales;

- The data are the ones strictly necessary to provide,
- Reporting,
- Testing,
- Training,
- Incidents,
- Certifications,
- Audits,
- Administration.
- The process of conducting an automated document check is a fair use of personal data and it is lawful under the guidelines of GDPR.

PROPORTIONALITY

Viridian maintains the ability to process personally identifiable information to manage the activities and to then review the outcomes of the process itself, in the form of reports, KPI's and test results in order to have an audit trail that complies with contractual obligated services.

Viridian believes that the personally identifiable information sent to Viridian by its clients is proportional for its intended use, since the information collected is what is strictly necessary to manage the process.

In the following table it is explained for which purposes each piece of information is stored in Viridian. Surely, some of them are necessary for more than one reason.

PRIVACY & GDPR POLICY

	Unique identification	Reporting	Notices to users	Compliance
Full Name		X	X	X
Company		X		X
Location and sublocation				X
Payroll number	X			X
Company role				X
E-Mail	X		X	
Phone	X		X	
Badge details	X			X
Username				X

Table 1 - Data and purposes

8. OUR DETAILS

8.1.
VIRIDIAN service is owned and operated by ICTS UK.

8.2.
We are registered in South Block, Entrance D, Tavistock House, Tavistock Square, London, WC1H 9LG. UK.

8.3.
You can contact us:
(a) by post, to the postal address given above; (b) using our website contact form;
(c) by email, using the email address viridian.support@ictseurope.com

PRIVACY & GDPR POLICY

9. DATA PROTECTION OFFICER

9.1.

Our data protection officer's contact details are; DPO@icts.co.uk.