

VIRTUS Data Centres

SITE ACCESS PRIVACY NOTICE

Table of Contents

TOPIC	PAGE
Key summary	2
About us and this notice	2
Useful words and phrases	3
What information do we collect?	5
Why do we process your personal data?	5
How is processing your data lawful?	7
Who will have access to your personal data?	8
When will we delete your data?	9
Your rights	10

VIRTUS Public				
Author:	Kyle Morrison	Release Date:	17/10/2023	
			Major Version	Minor Version
Approved:	David Tait / Helen Kinsman	Document Control:	1.	4

ABOUT US and THIS NOTICE

What does this notice apply to?

This Privacy Notice describes we process personal data in order to control access to our data centre premises. Read it to find out what we process, why we need it and your rights.

Which companies give this Privacy Notice?

Each of VIRTUS' group companies listed below is a 'controller' for the purposes of the General Data Protection Regulation (EU) 2016/679 when it processes personal data covered by this Privacy Notice (referred to as "we" or "us").

- Enfield DC Service Company Limited
- VIRTUS Enfield LLP
- VIRTUS Hayes Limited
- VIRTUS Slough Limited
- VIRTUS LONDON5 Limited
- VIRTUS LONDON6 Limited
- VIRTUS LONDON7 Limited
- VIRTUS LONDON8 Limited
- VIRTUS LONDON9 Limited
- VIRTUS LONDON10 Limited
- VIRTUS LONDON11 Limited

How to contact us

If you need to contact us about this Privacy Notice, use the details below

- Data Protection Officer: **Helen Kinsman**
- Address: **20 Balderton Street, LONDON, W1K 6TN**
- Telephone number: **+44 (0) 20 7499 1300**
- Email: privacy@virtusdcs.com

If you would like this Privacy Notice in another format (for example: audio, large print, braille), please contact us.

Changes to this Privacy Notice

A summary of the Privacy Notice will be provided to you when you sign in to enter one of our data centres. The full version, which we may update from time to time, will be available on our website at <https://virtusdatacentres.com/> or upon request within the data centres. Note that this privacy notice will be in addition to the privacy notice already on the website which relates to personal data collected through the website. Changes will be drawn to your attention the next time you enter the data centre and supplied in amended customer operations manuals.

VIRTUS Public				
Author:	Kyle Morrison	Release Date:	17/10/2023	
			Major Version	Minor Version
Approved:	David Tait / Helen Kinsman	Document Control:	1.	4

VIRTUS Public				
Author:	Kyle Morrison	Release Date:	17/10/2023	
		Document Control:	Major Version	Minor Version
Approved:	David Tait / Helen Kinsman		1.	4

USEFUL WORDS AND PHRASES

Please familiarise yourself with the following words and phrases (used in **bold**) as they have particular meanings in the **Data Protection Laws** and are used throughout this Privacy Notice:

Term	Definition
controller	This means any person who determines the purposes for which, and the manner in which, any personal data is processed .
Data Protection Laws	This means the laws which govern the handling of personal data . This includes the General Data Protection Regulation (EU) 2016/679 and any other national laws implementing that Regulation or related to data protection.
data subject	The person to whom the personal data relates.
ICO	This means the UK Information Commissioner's Office which is responsible for implementing, overseeing, and enforcing the Data Protection Laws .
personal data	<p>This means any information from which a <u>living individual</u> can be identified.</p> <p>This will include information such as telephone numbers, names, addresses, e-mail addresses, photographs, and voice recordings. It will also include expressions of opinion and indications of intentions about data subjects (and their own expressions of opinion/intentions).</p> <p>It will also cover information which on its own does not identify someone, but which would identify them if put together with other information which we have or are likely to have in the future.</p>
processing	<p>This covers virtually anything anyone can do with personal data, including:</p> <ul style="list-style-type: none"> • obtaining, recording, retrieving, consulting or holding it; • organising, adapting or altering it; • disclosing, disseminating, or otherwise making it available; and • aligning, blocking, erasing, or destroying it.
processor	This means any person who processes the personal data on behalf of the controller.

VIRTUS Public				
Author:	Kyle Morrison	Release Date:	17/10/2023	
Approved:	David Tait / Helen Kinsman	Document Control:	Major Version	Minor Version
			1.	4

Term	Definition
special categories of data	<p>This means any information relating to:</p> <ul style="list-style-type: none"> • racial or ethnic origin. • political opinions. • religious beliefs or beliefs of a similar nature. • trade union membership. • physical or mental health or condition. • sexual life; or • genetic data or biometric data for the purpose of uniquely identifying you.

VIRTUS Public				
Author:	Kyle Morrison	Release Date:	17/10/2023	
			Major Version	Minor Version
Approved:	David Tait / Helen Kinsman	Document Control:	1.	4

WHAT PERSONAL DATA DO WE COLLECT?

We collect the following **personal data** in the course of your entering and moving around within our data centres:

- Names
- Digital photographs
- Access biometrics such as fingerprints or palm-prints
- CCTV surveillance footage

We do not collect any information from third parties or any **special categories of data**, unless you make certain **special categories of data** apparent in your appearance which could then be captured on CCTV or photographs such as clothing typically associated with a religion.

WHY DO WE PROCESS YOUR PERSONAL DATA?

It is central to our commitments to our clients that we maintain security at our data centres, including protecting client equipment, protecting critical shared infrastructure and controlling authorised site personnel.

Specifically, **personal data** will be used for the following purposes:

- **Names and identification documentation:**

In order to grant you access to a data centre, we need to verify who you are. We do this by confirming your name against a client authorised access list or VIRTUS-approved access request. Further verification is required by authenticating your name on government-issued identification such as a passport, driving licence or national identity. Such identification is NOT copied but is examined under ultra violet light to verify that they incorporate the anti-forgery ultra violet ink as designed.

- **Digital photographs and access biometrics:**

Photographs are printed onto an access card to verify who you are whilst on site. Biometrics are registered against your access card to permit access to controlled areas such as client restricted areas or areas which house critical infrastructure.

- **CCTV surveillance footage:**

We use CCTV cameras throughout the data centre (other than single use customer halls), and the car parks to facilitate security measures and support our guarding staff. Live footage is monitored by our guarding contractors so that they can monitor the whole site from a single, secure location. Other than the live monitoring, footage will only be viewed by VIRTUS-Security and their contracted Vendor-Security, to prove the system is functional, investigate security-related incidents, activity in contravention of our site rules or unlawful activity. Footage will only be released to authorities where required for investigatory purposes or to exercise or defend VIRTUS' legal rights.

VIRTUS Public				
Author:	Kyle Morrison	Release Date:	17/10/2023	
			Major Version	Minor Version
Approved:	David Tait / Helen Kinsman	Document Control:	1.	4

HOW IS PROCESSING YOUR PERSONAL DATA LAWFUL?

We are allowed to **process** your **personal data** for the following reasons and on the following legal bases:

- Legitimate Interests:**

We are permitted to **process** your **personal data** if it is based on our 'legitimate interests' i.e. we have good, sensible, practical reasons for **processing** your **personal data** which is in the interests of VIRTUS.

It is in our legitimate interest, and the interest of our clients, to maintain the security of our data centres by identifying all individuals who access it and, given that we operate data centres shared by multiple clients, to monitor where people go within our data centres to check that they only access the areas that they are authorised to access. For those accessing restricted client areas or areas which house critical infrastructure, we obtain more data, such as biometric data, to make regular access quicker, easier and more secure.

We may also **process** this data in order to exercise or defend our legal rights.

We have considered the impact on the interests and rights of those who access our data centres and have placed appropriate safeguards to ensure that the intrusion to privacy is reduced as much as possible. The access card that you use in the data centre does not store your name. We register your name against an access card number so that if the card is stolen, lost or even counterfeited, your name is not associated with the biometric details on the card.

You can object to **processing** that we carry out on the grounds of legitimate interests. See the section headed "[Your Rights](#)" to find out how.

- Special categories of data made public by you**

If you make certain **special categories of data** apparent in your appearance which could then be captured on CCTV or photographs such as clothing typically associated with a religion, we will **process** that data for the purposes set out above.

VIRTUS Public				
Author:	Kyle Morrison	Release Date:	17/10/2023	
			Major Version	Minor Version
Approved:	David Tait / Helen Kinsman	Document Control:	1.	4

WHO WILL HAVE ACCESS TO YOUR PERSONAL DATA?

The table below lists some of our key service providers that act as our **processors** who will have access to your **personal data**. This provider performs standard, enterprise IT services which require 'passive' processing in the form of providing security support, none of which requires them to actively deal with the data.

Who information is shared with: processors
ICTS Security Bouygues

We will also share your **personal data** with the police, other law enforcement agencies or regulators where we are required by law to do so.

Transfers of your personal data outside the EEA

VIRTUS does not transfer your **personal data** outside the European Economic Area.

How we keep your personal data secure

We strive to implement appropriate technical and organisational measures in order to protect your **personal data** against accidental or unlawful destruction, accidental loss or alteration, unauthorised disclosure or access and any other unlawful forms of **processing**. We aim to ensure that the level of security and the measures adopted to protect your **personal data** are appropriate for the risks presented by the nature and use of your **personal data**. We follow recognised industry practices for protecting our IT environment and physical facilities and are certified to **ISO27001:2022**.

VIRTUS Public				
Author:	Kyle Morrison	Release Date:	17/10/2023	
			Major Version	Minor Version
Approved:	David Tait / Helen Kinsman	Document Control:	1.	4

WHEN WILL WE DELETE YOUR DATA?

The following categories of **personal data** and **special categories of data** will be kept for the following periods.

Personal data	Retention period
Identification documents	Not retained – only viewed to verify identity on entry to the data centres
Names and digital photographs	As long as specified under the requirements for access OR 2 years – whichever is sooner. After 2 years (if required under the requirements for access) names and digital photographs will be manually re-instated on access cards.
Access biometrics	As long as specified under the requirements for access OR 2 years – whichever is sooner. After 2 years (if required under the requirements for access) biometrics will be manually re-instated on access cards.
CCTV surveillance footage	This is determined based on assessment of risk and accordance with Data Protection obligations.

VIRTUS Public				
Author:	Kyle Morrison	Release Date:	17/10/2023	
			Major Version	Minor Version
Approved:	David Tait / Helen Kinsman	Document Control:	1.	4

YOUR RIGHTS

As a **data subject**, you have the following rights under the **Data Protection Laws**:

- the right to object to **processing** of your **personal data**;
- the right of access to **personal data** relating to you (known as data subject access request);
- the right to correct any mistakes in your information;
- the right to prevent your **personal data** being processed; and
- the right to erasure.

These rights are explained in more detail below. If you want to exercise any of your rights, please contact us (please see "How to contact us").

We will respond to any rights that you exercise within a month of receiving your request, unless the request is particularly complex, in which case we will respond within three months.

Please be aware that there are exceptions and exemptions that apply to some of the rights which we will apply in accordance with the **Data Protection Laws**.

Right to object to processing of your personal data

You may object to us **processing** your **personal data** where we rely on a legitimate interest as our legal grounds for **processing**.

If you object to us **processing** your **personal data**, we must demonstrate compelling grounds for continuing to do so. We believe we have demonstrated compelling grounds in the section headed "How is processing your personal data lawful". Please note that if you object, you will not be permitted access to the data centres.

Right to access personal data relating to you

You may ask to see what **personal data** we hold about you and be provided with:

- a copy of the personal data;
- details of the purpose for which the personal data is being or is to be **processed**;
- details of the recipients or classes of recipients to whom the personal data is or may be disclosed, including if they are overseas and what protections are used for those overseas transfers;
- the period for which the personal data is held (or the criteria we use to determine how long it is held);

VIRTUS Public				
Author:	Kyle Morrison	Release Date:	17/10/2023	
			Major Version	Minor Version
Approved:	David Tait / Helen Kinsman	Document Control:	1.	4

- any information available about the source of that data; and
- whether we carry out an automated decision-making, or profiling, and where we do information about the logic involved and the envisaged outcome or consequences of that decision or profiling.

To help us find the information easily, please provide us as much information as possible about the type of information you would like to see.

Right to correct any mistakes in your information

You can require us to correct any mistakes in your information which we hold. If you would like to do this, please let us know what information is incorrect and what it should be replaced with.

Right to restrict processing of personal data

You may request that we stop **processing** your **personal data** temporarily if:

- you do not think that your data is accurate. We will start **processing** again once we have checked whether or not it is accurate;
- the **processing** is unlawful but you do not want us to erase your data;
- we no longer need the **personal data** for our **processing**, but you need the data to establish, exercise or defend legal claims; or
- you have objected to **processing** because you believe that your interests should override our legitimate interests.

Right to forget

You can ask us to erase your **personal data** where:

- you do not believe that we need your data in order to **process** it for the purposes set out in this Privacy Notice;
- you object to our **processing** and we do not have any legitimate interests that mean we can continue to **process** your data; or
- your data has been **processed** unlawfully or have not been erased when it should have been.

VIRTUS Public				
Author:	Kyle Morrison	Release Date:	17/10/2023	
			Major Version	Minor Version
Approved:	David Tait / Helen Kinsman	Document Control:	1.	4

What will happen if your rights are breached?

You may be entitled to compensation for damage caused by contravention of the **Data Protection Laws**.

VIRTUS maintain Information Security Breach and Incident Management Systems to; 1) contain and recover information, 2) assess the risks, 3) provide breach notifications, and 4) evaluate and effectively respond.

Complaints to the regulator

It is important that you ensure you have read this Privacy Notice - and if you do not think that we have **processed** your data in accordance with this notice - you should let us know as soon as possible. You may also complain to the **ICO**. Information about how to do this is available on his website at www.ico.org.uk.

VIRTUS Public				
Author:	Kyle Morrison	Release Date:	17/10/2023	
			Major Version	Minor Version
Approved:	David Tait / Helen Kinsman	Document Control:	1.	4