

GDPR

Date: 01/03/2018

Description: Published

ISO: QD618 Rev 1.0

What is GDPR?.....page 3
 GDPR: 8 Individual Rights.....page 4

Where is Data Stored?.....page 5

Data Protection & Security.....page 6

Privacy Policy.....page 7

What is GDPR?

The EU General Data Protection Regulation (GDPR), replaces the Data Protection Directive 95/46/EC. GDPR seeks to create a harmonised data protection law framework across the EU and aims to give citizens back the control of their personal data, whilst imposing strict rules on those hosting and 'processing' this data, anywhere in the world. The Regulation also introduces rules relating to the free movement of personal data within and outside the EU.

GDPR is designed to give individuals better control over their personal data and establish one single set of data protection rules across Europe.

When companies obtain data from an individual, some of the areas that must be made clear to the data subject are:

- The identity and contact details of the organisation behind the data request
- The purpose of acquiring the data and how it will be used
- Whether the data will be transferred internationally
- The period for which the data will be stored
- The individual's right to access, rectify or erase the data
- The individual's right to withdraw consent at any time
- The individual's right to lodge a complaint

GDPR regulations specify that you must:

- **Improve** security measures to protect personal data – Encryption, advanced firewalls and software protection are recommended throughout the regulation and widely agreed to be the best data security measure.
- **Implement** staff training and have policies and procedures in place – in order to show that you have taken reasonable steps to avoid a data breach, and what to do if one occurs.
- **Notify** affected parties in the event of a personal data breach - Has to be done without undue delay. If you can prove the data was encrypted and protected you may not need to notify the individuals concerned.
- **Pay** fines in the event of a personal data breach - If the data was encrypted and protected it's highly likely that no fines will be imposed.

GDPR: 8 Individual Rights that any person, that you store data for, can request:

The Right to be Informed:

As a business you are required to provide 'fair processing information' about an individual's personal data. This will generally be covered under your privacy policy. You will need to be very transparent on how you intend to use the personal data that you collect and store.

The Right of Access:

An individual has the right to access the personal data you store and any supplementary data. This allows the individual to be aware of what data is being held and verify the lawfulness of the processing. This data must be provided free of charge and without delay, at the latest within one month of the request.

The Right to Rectification:

Individuals can request to have an inaccurate or incomplete data rectified. It is your business responsibility to inform any third parties you have disclosed the information to of these amends. You must respond to the request with one month.

The Right to Erasure:

Also known as the 'right to be forgotten'. The general principle here is that the individual may request the deletion or removal of their personal data where there is no compelling reason for its continued processing. Whilst not an absolute right, it applies where the personal data is no longer necessary in relation to the original purpose, the individual withdraws consent, the individual objects to the processing, the data is unlawfully processed, it is a legal obligation, or the data processed is in relation to the offer of information society services to a child. You must also inform any third parties you have disclosed the personal data to.

The Right to Restrict Processing:

Individuals have the right to block or suppress the processing of their personal data. Your business may continue to store the personal data; however, you may not process it any further. The personal data that is stored should be reviewed and only the information required to ensure that the restriction is respected in future may be retained. Again, you must notify any third parties that you have disclosed data to.

The Right to Data Portability:

Individuals have the right to obtain and reuse their personal data for the own purposes across different services. Your business must supply their personal data in a structured, commonly used and machine-readable form which will allow other organisations to use the data. You must respond to this request without delay and within one month.

The Right to Object:

Individuals have the right to object to processing of their personal data based on legitimate interests or the performance of a task in the public interest of official authority, direct marketing, and processing for purposes of scientific/historical research and statistics. Your business must inform individuals of their right to object at the point of first communication and it should be included within your privacy policy.

Rights in Relation to Automated Decision Making and Profiling:

Individuals have the right not to be subject to a decision when it is based on automated processing and it produces a legal effect or similarly significant effect on the individual. The GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention. When your business is processing any personal data for profiling, you must ensure that appropriate safeguards have been put in place.

Where is Data Stored?

All hardware and applications used to process, transmit or store users data is housed in our 3 ISO27001 accredited, highly secure data centres, which are fully firewalled and securely manned 24/7.

- Custodian, Maidstone
- 4D, Surrey
- Everest, Reading

Data Centre Summary:

To ensure a business grade industry leading level of reliability and service all of the VSL Cloud services are supported by enterprise-class equipment and two geographically diverse ISO accredited UK based Data Centres.

Locations:

The location of the Data Centres we use is key to our performance and ultimately the aggressive service levels we want to offer. That is why we chose Custodian DC in Maidstone Kent, 4D in West Byfleet Surrey and Everest in Reading. All sites are close by and quickly accessible by either our UK offices. This accessibility is critical to ensure a timely response to any customer DR scenario. Another reason for their suitability is that they are situated just minutes off both the M20, M25 and the M4 which makes them highly accessible what ever the weather.

Round the Clock Accessibility:

All Data Centres provide VSL with 24 hour access. Physical Security Both Data Centres are monitored by CCTV surveillance around the clock. They have electronic access control through a single point of entry and operate fenced perimeters.

Digital Security:

Each data centre is protected by multiple firewalls and directly linked to a high-speed, resilient hosting network. This backbone LAN infrastructure is fed by multiple ISPs to ensure system integrity and availability at all times.

Resilience & Failover:

To guarantee reliability of service, each data set is protected by data centre two locations, each acting as primary and secondary storage to ensure resilience and ultimate load balancing. Data stored in the primary data arrays are automatically mirrored to a second data centre - an exact replica with the same security features as the primary array. This infrastructure moves to deliver a complete failover environment and absolute reliability.

Accreditations:

All data centres used by VSL are ISO27001 accredited. Certificates available via the following links:



<https://www.vsl-net.com/pdfs/4dISO27001Cert.pdf>

<https://www.vsl-net.com/pdfs/CustISO27001Cert.pdf>

For more information please see: <https://www.vsl-net.com/pdfs/DataCentreOverview.pdf>

Data Protection & Security

Vitanium Systems Limited are an ICO (Information Commissioner's Office) registered Company. ICO Data Protection Registration Reference: ZA202119

At VSL we are very conscious of our need to comply to the Data Protection Act 1998 and as a UK company we follow the guidelines provided by the Information Commissioners Office, which states:

Anyone who processes personal information must comply with eight principles, which make sure that personal information is:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than is necessary
- Processed in line with the users' rights
- Secure
- Not transferred between locations without adequate protection

With this in mind, all VSL staff are trained on compliance to the Data Protection Act and, in particular, the eight principles above.

All control panels are password protected and accessible over 128bit Secure Socket Layers (SSL) to give users of VSL services added confidence that any sensitive information stored on their behalf by VSL is safe and highly secure.

When providing support VSL are mindful of email sensitivity and will confirm first whether we have permission to read any email / data content, if required as part of the support.

All hardware and applications used to process, transmit or store users email / data are housed in multiple ISO27001 accredited, highly secure data centres, which are fully firewalled and securely manned 24/7.

For more information about our data centres please ask your VSL sales contact for the appropriate document

Privacy Policy: Overview

Security of Personal Information:

We will take reasonable technical and organisational precautions to prevent the loss, misuse or alteration of your personal information.

We will store all the personal information you provide on our secure password and firewall-protected servers.

All electronic financial transactions entered through our website will be protected by encryption technology.

You acknowledge that the transmission of information over the internet is inherently insecure, and we cannot guarantee the security of data sent over the internet.

You are responsible for keeping the password you use for accessing our website or services confidential; we will not ask you for your password (except when you log in to our website).

Your Rights:

You may instruct us to provide you with any personal information we hold about you; provision of such information will be subject to:

- the supply of appropriate evidence of your identity

We may withhold personal information that you request to the extent permitted by the law.

You may instruct us at any time not to process your personal information for marketing purposes.

In practice, you will usually either expressly agree in advance to our use of your personal information for marketing purposes. Or we will provide you with an opportunity to opt out of the use of your personal information for marketing purposes.

Data Protection Registration:

We are registered as a data controller with the UK Information Commissioner's Office (ICO)

Our Data Protection registration number is: **ZA202119**

For more information please visit: <https://vsl-net.com/pdfs/privacyPolicyQD117.pdf>

Contact us

Vitanium Systems Limited trading as VSL

4 Atlantic Square,

Station Road,

Witham, Essex,

CM8 2TL

Tel: 0845 258 1500 option 1 E-mail: info@vsl-net.com

Vitanium Systems Limited is an ISO9001 accredited company registered in England and Wales. Company Number: 4976354.

Registered Office: 4 Atlantic Square, Station Road, Witham, Essex, CM8 2TL

VAT Reg. No: 831 8525 27