VTSL Data Protection Policy & GDPR Compliance Information

version 1 updated 26.04.2018

www.vtsl.net
VTSL LTD 5 NICKOLS WALK, LONDON, SW18 1BZ

Table of Contents

Introduction

VTSL Ltd is committed to protecting the rights and freedoms of data subjects, and safely and securely processing their data in accordance with all of our legal obligations.

We hold personal data about our employees, clients, suppliers and other individuals for a variety of business purposes.

This policy sets out how we seek to protect personal data and ensure that our staff understand the rules governing their use of the personal data to which they have access in the course of their work. In particular, this policy requires staff to ensure that the Data Protection Officer (DPO) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

Definitions

Business purposes	The purposes for which personal data may be used by us: Delivering our service, personnel, administrative, financial, regulatory, payroll and business development purposes. Specifically, 'business purposes' includes the following: - *Delivering our services including connectivity, telephony, mobile and any other services detailed on a client's Order Form* - *Compliance with our legal, regulatory and corporate governance obligations and good practice* - *Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests* - *Ensuring business policies are adhered to (such as policies covering email and internet use)* - *Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, security vetting, credit scoring and checking* - *Investigating complaints* - *Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments* - *Monitoring staff conduct, disciplinary matters* - *Marketing new products or services* - *Improving services*

Personal data	'Personal data' means any information relating to an identified or identifiable natural person ('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. *Personal data we gather may include but is not necessarily limited to: email address, home address, mobile phone number, phone call records, call recordings (if you have subscribed to this service), website visits, website downloads, website form entry and interactions with VTSL (emails and phone calls, including call recordings of calls made to or received from VTSL)*
Special categories of personal data	Special categories of data include information about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings, and genetic and biometric information —any use of special categories of personal data should be strictly controlled in accordance with this policy.
Data controller	'Data controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by law.
Data processor	'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Processing	'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Supervisory authority	This is the national body responsible for data protection. The supervisory authority for our organisation is Ofcom in the UK and ComReg in Ireland. VTSL are also members of ITSPA (Internet Telephony Service Providers Association).

Scope

This policy applies to all staff, who must be familiar with this policy and comply with its terms. This policy is supplemented by VTSL's Internal Data Protection Policy, which all staff are required to read and agree to.

We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

Who is responsible for this policy?

As our data protection officer (DPO), Nicola White has overall responsibility for the day-to-day implementation of this policy. You should contact the DPO for further information about this policy if necessary.

VTSL's Data Protection Officer: Nicola White
Email: nwhite@vtsl.net
Phone: 020 7078 3200

The Principles

VTSL shall comply with the principles of data protection (the Principles) enumerated in the EU General Data Protection Regulation (GDPR). We will make every effort possible in everything we do to comply with these principles. The Principles are:

1. Lawful, fair and transparent

Data collection must be fair, for a legal purpose and we must be open and transparent as to how the data will be used.

2. Limited for its purpose

Data can only be collected for a specific purpose.

3. Data minimisation

Any data collected must be necessary and not excessive for its purpose.

4. Accurate

The data we hold must be accurate and kept up to date.

5. Retention

We cannot store data longer than necessary.

6. Integrity and confidentiality

The data we hold must be kept safe and secure.

Accountability and Transparency

VTSL ensures accountability and transparency in all our use of personal data.

To comply with data protection laws and the accountability and transparency Principle of GDPR, VTSL has done the following:

1. Conducted a full privacy impact assessment & created a data map
2. Assessed data security measures
3. Reviewed Breach Notification processes
4. Reviewed and updated VTSL's Contracts
5. Reviewed and updated VTSL's policies
6. Built awareness about correct data protection with employees
7. Appointed a Data Protection Officer
8. Reviewed processes for responding to subject access requests
9. Incorporated privacy considerations in all new product development processes
10. Reviewed all record keeping systems

VTSL employees are required to demonstrate a full understanding of the responsibilities they hold that will ensure VTSL meets its data protection obligations. All employees were required to attend *VTSL's Data Protection Workshop* in April 2018, outlining exactly what they are responsible for, and agree to VTSL's Internal Data Protection Policy.

Data Map

VTSL's Data Map outlines how data enters VTSL, where it resides, how it is transferred, how it is secured and the lawful reason for processing.

You may request a copy of VTSL's current data map by emailing datarequest@vtsl.net. Requests are fulfilled at VTSL's discretion.

Our Procedures

Fair and lawful processing

We must process personal data fairly and lawfully in accordance with individuals' rights under the first Principle. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening.

If we cannot apply a lawful basis (explained below), our processing does not conform to the first principle and will be unlawful, in which case it will not be processed. Data subjects have the right to have any data unlawfully processed erased.

Controlling vs. processing data

VTSL is classified as a data controller and data processor. We maintain our appropriate registration with the Information Commissioners Office in order to continue lawfully controlling and processing of data.

As a data processor, we must:

- Not use a sub-processor without written authorisation of the data controller
- Co-operate fully with the ICO or other supervisory authority
- Ensure the security of the processing
- Keep accurate records of processing activities
- Notify the controller / DPO of any personal data breaches

If you are in any doubt about how we handle data, contact the DPO for clarification.

Lawful basis for processing data

All data processed by VTSL has a lawful basis approved by our DPO. VTSL ensures that at least one of the following conditions applies whenever we process personal data:

1. **Consent**

We hold recent, clear, explicit, and defined consent for the individual's data to be processed for a specific purpose.

2. **Contract**

The processing is necessary to fulfil or prepare a contract for the individual.

3. **Legal obligation**

We have a legal obligation to process the data (excluding a contract).

4. **Vital interests**

Processing the data is necessary to protect a person's life or in a medical situation.

5. **Public function**

Processing necessary to carry out a public function, a task of public interest or the function has a clear basis in law.

6. **Legitimate interest**

The processing is necessary for our legitimate interests. This condition does not apply if there is a good reason to protect the individual's personal data which overrides the legitimate interest.

For all existing data processing activities, the condition for lawfulness is clearly shown in our Data Map. For all new data processing activities we will a) establish that processing is necessary, and b) ensure that there is at least one lawful basis that applies to the processing purpose. This will be documented and added to VTSL's Data Map.

All individuals with data processed or held by VTSL are informed of the lawful basis for processing their data, as well as the intended purpose. This occurs through our Privacy Notices, Terms & Conditions, VTSL Data Protection Policy & GDPR Compliance document and VTSL Internal Data Protection Policy.

Special Categories of Personal Data

What are special categories of personal data?

Previously known as sensitive personal data, this means data about an individual which is more sensitive, so requires more protection. This type of data could create more significant risks to a person's fundamental rights and freedoms, for example by putting them at risk of unlawful discrimination. The special categories include information about an individual's:

- race
- ethnic origin
- politics
- religion
- trade union membership
- genetics
- biometrics (where used for ID purposes)
- health
- sexual orientation

VTSL does not process any special category personal data.

Responsibilities

Below we have listed VTSL's responsibilities that ensure data is appropriately controlled and processed.

VTSL's responsibilities:

- Analysing and documenting the type of personal data we hold
- Checking procedures to ensure they cover all the rights of the individual
- Identify the lawful basis for processing data
- Ensuring consent procedures are lawful
- Implementing and reviewing procedures to detect, report and investigate personal data breaches
- Store data in safe and secure ways
- Assess the risk that could be posed to individual rights and freedoms should data be compromised

VTSL employee responsibilities:

- Fully understand data protection obligations
- Check that any data processing activities you are dealing with comply with our policy and are justified
- Do not use data in any unlawful way
- Do not store data incorrectly, be careless with it or otherwise cause us to breach data protection laws and our policies through your actions
- Comply with this policy and VTSL's Internal Data Protection Policy at all times
- Raise any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this policy or our legal obligations without delay

Responsibilities of the Data Protection Officer:

- Keeping the board updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies on a regular basis
- Arranging data protection training and advice for all staff members and those included in this policy
- Answering questions on data protection from staff, board members and other stakeholders
- Responding to individuals such as clients and employees who wish to know which data is being held on them by us
- Checking and approving with third parties that handle the company's data any contracts or agreement regarding data processing

Responsibilities of the IT Manager:

- Ensure all systems, services, software and equipment meet acceptable security standards
- Checking and scanning security hardware and software regularly to ensure it is functioning properly
- Researching third-party services, such as cloud services the company is considering using to store or process data

Responsibilities of the Marketing Manager:

- Approving data protection statements attached to emails and other marketing copy
- Addressing data protection queries from clients, target audiences or media outlets

- Coordinating with the DPO to ensure all marketing initiatives adhere to data protection laws and the company's Data Protection Policy

Accuracy and relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. Once a request for a correction is made, VTSL guarantees that the correction will be made within 72 hours, and will be checked and documented by the DPO.

Data security

General systems & cloud services:

VTSL ensures all data we hold either on our own systems, or on cloud-based software, is as secure as possible against loss or misuse. This entails using two factor authentication, encryption, secure data centres, password managers and security software in addition to regular staff training.

We also do regular security reviews of all VTSL systems and apply patches for security issues.

Third parties:

VTSL only passes data to third parties as necessary to provide our services, or communications about our services. All third parties have been vetted for adequate security and checked for compliance with the GDPR as part of our security measures review.

Call recordings:

There is no direct access from the internet to any of the VTSL call recording storage systems. Access to all storage systems is controlled by means of VPN and individual SSH authentication keys.

Recordings are accessible for the customers on the VTSL web portal anytime. Deleting them is a request VTSL fulfils within 72 hours.

Storing data securely

- VTSL does not hold any data on paper. All personal data is held in secure, cloud-based systems that only VTSL authorised staff have access to.
- Data stored on VTSL computers is protected by strong passwords that are changed regularly. Most VTSL systems require two-factor authentication, including email.

- Data stored on CDs or memory sticks must be encrypted or password protected and locked away securely when they are not being used.
- All VTSL's cloud-based data storage systems and applications have been approved by the DPO.
- Servers containing personal data are kept in a secure location, not in VTSL's general office space.
- Data is regularly backed up in line with VTSL's backup procedures.
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones.
- All servers containing sensitive data must be approved and protected by security software.

Data retention

We will retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but each case will be determined in a manner consistent with current regulations.

For call recordings, VTSL stores the recordings as long as the customer is with VTSL. Once the organisation has left VTSL, the call recordings are deleted.

For emails, VTSL retains archives for 6 years before the email is deleted.

Transferring data internationally

VTSL does not transfer personal data abroad, or anywhere else outside of normal rules and procedures. In the unusual event that this is necessary, express permission from the DPO would be obtained.

Rights of individuals

Individuals have rights to their data which VTSL respects and complies with to the best of our ability. We ensure individuals can exercise their rights in the following ways:

1. Right to be informed

- VTSL's Privacy Notice is concise, transparent, intelligible and easily accessible, free of charge, and written in clear and plain language.
- VTSL keeps a record of how we use personal data to demonstrate compliance with the need for accountability and transparency.

2. Right of access

- Individuals may access their personal data and supplementary information with a written request. Written requests should be made to datarequests@vtsl.net.

- VTSL makes individuals aware of the lawfulness of the processing activities through the Privacy Notices we provide.

3. Right to rectification

- VTSL will rectify or amend the personal data of the individual if requested because it is inaccurate or incomplete.
- This will be done within 72 hours of the request. Requests should be sent to datarequests@vtsl.net.

4. Right to erasure

- VTSL will delete or remove an individual's data if requested and there is no compelling reason for its continued processing.

5. Right to restrict processing

- VTSL will comply with any request to restrict, block, or otherwise suppress the processing of personal data. Requests should be sent to datarequest@vtsl.net.
- VTSL is permitted to store personal data if it has been restricted, but not process it further. We must retain enough data to ensure the right to restriction is respected in the future.

6. Right to data portability

- VTSL will supply individuals with their data so that they can reuse it for their own purposes or across different services.
- VTSL will provide it in a commonly used format and send it directly to another controller if requested.

7. Right to object

- VTSL will respect the right of an individual to object to data processing based on legitimate interest or the performance of a public interest task.
- VTSL will respect the right of an individual to object to direct marketing, including profiling.
- VTSL will respect the right of an individual to object to processing their data for scientific and historical research and statistics.

8. Rights in relation to automated decision making and profiling

- VTSL will respect the rights of individuals in relation to automated decision making and profiling.
- Individuals retain their right to object to such automated processing, have the rationale explained to them, and request human intervention.

Privacy notices

VTSL supplies a privacy notice at the time the data is obtained if obtained directly from the data subject. If the data is not obtained directly from the data subject, the privacy notice is provided within one month.

If the data is being used to communicate with the individual, then the privacy notice will be supplied at the latest when the first communication takes place.

If for some reason VTSL is required to disclose information to another party, a privacy notice will be supplied prior to the data being disclosed.

The following information is included in VTSL's privacy notices:

- Identification and contact information of the data controller and the data protection officer
- The purpose of processing the data and the lawful basis for doing so
- The legitimate interests of the controller or third party, if applicable
- The right to withdraw consent at any time, if applicable
- The category of the personal data (only for data not obtained directly from the data subject)
- Any recipient or categories of recipients of the personal data
- The retention period of the data or the criteria used to determine the retention period, including details for the data disposal after the retention period
- The right to lodge a complaint with the ICO, and internal complaint procedures
- The source of the personal data, and whether it came from publicly available sources (only for data not obtained directly from the data subject)
- Any existence of automated decision making, including profiling and information about how those decisions are made, their significances and consequences to the data subject
- Whether the provision of personal data is part of a statutory of contractual requirement or obligation and possible consequences for any failure to provide the data (only for data obtained directly from the data subject)

Subject Access Requests

What is a subject access request?

An individual has the right to receive confirmation that their data is being processed, access to their personal data and supplementary information.

How we deal with subject access requests

VTSL will provide the individual with a copy of the information the request, free of charge. This will occur within 72 hours of the request. We endeavour to provide data subjects access to their information in commonly used electronic formats. The process for handling data requests is as follows:

- Email datarequest@vtsl.net or support@vtsl.net with details of your written request.

- Please include the name of your organisation, the name of the individual, your phone number, the name of your organisations DPO or person responsible for data protection, and the data you would like to have delelted.

- You will then receive confirmation that we have received your request, and within 72 hours confirmation that your request has been fulfilled.

If complying with the request is complex or numerous, the deadline for fulfilling the request will be one month.

VTSL can refuse to respond to certain requests, and can, in circumstances of the request being manifestly unfounded or excessive, charge a fee. If the request is for a large quantity of data, we can request the individual specify the information they are requesting. This can only be done with express permission from the DPO.

Once a subject access request has been made, VTSL will not change or amend any of the data that has been requested.

Data portability requests

VTSL will provide the data requested in a structured, commonly used and machine-readable format. This would normally be a CSV file, although other formats are acceptable. We will provide this data either to the individual who has requested it, or to the data controller they have requested it be sent to. This is done free of charge and without delay, and no later than one month from the time of request. This can be extended to two months for complex or numerous requests, but the individual must be informed of the extension within one month and permission must be granted from the DPO first.

Right to Erasure

What is the right to erasure?

Individuals have a right to have their data erased and for processing to cease in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected and / or processed
- Where consent is withdrawn
- Where the individual objects to processing and there is no overriding legitimate interest for continuing the processing

- The personal data was unlawfully processed or otherwise breached data protection laws
- To comply with a legal obligation
- The processing relates to a child

How we deal with the right to erasure

We can only refuse to comply with a right to erasure in the following circumstances:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

If personal data that needs to be erased has been passed onto other parties or recipients, VTSL will ensure they are contacted and informed of their obligation to erase the data. If the individual asks, we must inform them of those recipients.

The right to object

Individuals have the right to object to their data being used on grounds relating to their particular situation. We must cease processing unless:

- We have legitimate grounds for processing which override the interests, rights and freedoms of the individual.
- The processing relates to the establishment, exercise or defence of legal claims.

We must always inform the individual of their right to object at the first point of communication, i.e. in the privacy notice. We must offer a way for individuals to object online.

The right to restrict automated profiling or decision making

We may only carry out automated profiling or decision making that has a legal or similarly significant effect on an individual in the following circumstances:

- It is necessary for the entry into or performance of a contract.
- Based on the individual's explicit consent.
- Otherwise authorised by law.

In these circumstances, we must:

- Give individuals detailed information about the automated processing.
- Offer simple ways for them to request human intervention or challenge any decision about them.
- Carry out regular checks and user testing to ensure our systems are working as intended.

Third parties

Using third party controllers and processors

As a data controller and processor, we must have agreements in place with all third-party data controllers and processors that we use that ensure they are compliant with the existing regulations and that they have appropriate security measures to adequately protect the data we share with them.

As a data controller, we must only appoint processors who can provide sufficient guarantees under GDPR and that the rights of data subjects will be respected and protected.

As a data processor, we must only act on the documented instructions of a controller. We acknowledge our responsibilities as a data processor under GDPR and we will protect and respect the rights of data subjects.

Contracts

Our contracts comply with the standards set out by the ICO. Our contracts with data controllers and processors set out the subject matter and duration of the processing, the nature and stated purpose of the processing activities, the types of personal data and categories of data subject, and the obligations and rights of the controller.

At a minimum, our contracts must include terms that specify:

- Acting only on written instructions
- Those involved in processing the data are subject to a duty of confidence
- Appropriate measures will be taken to ensure the security of the processing
- Sub-processors will only be engaged with the prior consent of the controller and under a written contract
- The controller will assist the processor in dealing with subject access requests and allowing data subjects to exercise their rights under GDPR
- The processor will assist the controller in meeting its GDPR obligations in relation to the security of processing, notification of data breaches and implementation of Data Protection Impact Assessments
- Delete or return all personal data at the end of the contract
- Submit to regular audits and inspections, and provide whatever information necessary for the controller and processor to meet their legal obligations.
- Nothing will be done by either the controller or processor to infringe on GDPR.

Criminal Offence Data

VTSL does not carry out criminal record checks. Should we ever carry out a criminial record check in the future, we understand that we cannot keep a comprehensive register of criminal offence data. We also understand all data relating to criminal offences is considered to be a special category of personal data and must be treated as such.

Audits, Monitoring and Training

Data audits

VTSL conducts data audits annually, updating our Data Map and Register.

This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

Monitoring

All VTSL employees must adhere to our monitoring policies, and notify the DPO of any breaches.

Training

All VTSL employees receive adequate training on provisions of data protection law specific to their role. If they change roles or responsibilities, they are responsible for requesting new data protection training relevant to their new position or responsibilities.

If they require additional training on data protection matters, they can contact the DPO.

Reporting Breaches

Breach notification processes

In addition in to the security / network breach notification obligations in PECR and set out in the Ofcom Security Guidelines, any breach of this policy or of data protection laws must be reported as soon as practically possible to Ofcom, ComReg, the ICO and the data subjects. Our employees have been informed they must inform our DPO as they have become aware of a breach, so that the DPO can inform the other necessary parties.

With all data breaches, VTSL will:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of the compliance failure(s)
- Notify Ofcom or ComReg of any compliance failures that are material either in their own right or as part of a pattern of failures

Any member of staff who fails to notify of a breach, or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures will be liable to disciplinary action.

Breach notification to regulators

VTSL's DPO will report 'personal data breaches' to the ICO and Ofcom / ComrReg without undue delay and, where feasible, within 72 hours of becoming aware of the breach, unless the breach is unlikely to result in risk for the rights and freedoms of individuals. A personal data breach is defined quite widely to include: "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".

The notification will include the following information at a minimum:

- the nature of the breach
- the categories of data and number of people involved
- the approximate number of records
- the effect and remedial action taken by the VTSO an our DPO must be provided

Breach notification to data subjects

VTSL will notify affected individuals without undue delay if their rights and freedoms are put at high risk.

The notification will include the following information at a minimum:

- the nature of the breach
- details of the DPO
- the likely consequences
- the measures being taken to address the breach

VTSL could choose to not notify if one of the conditions below is met:

- the controller or DPO has implemented measures to protect the data, including those that render the data unintelligible, for example, encryption;
- the controller or DPO has taken measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise; or
- notifying data subjects would involve disproportionate effort, although in such circumstances a public communication is then envisaged

Failure to comply

We take compliance with this policy very seriously. Any employee who fails to comply with any requirement of this policy may be subject to disciplinary action, which may result in dismissal.