TRIALVIEW®

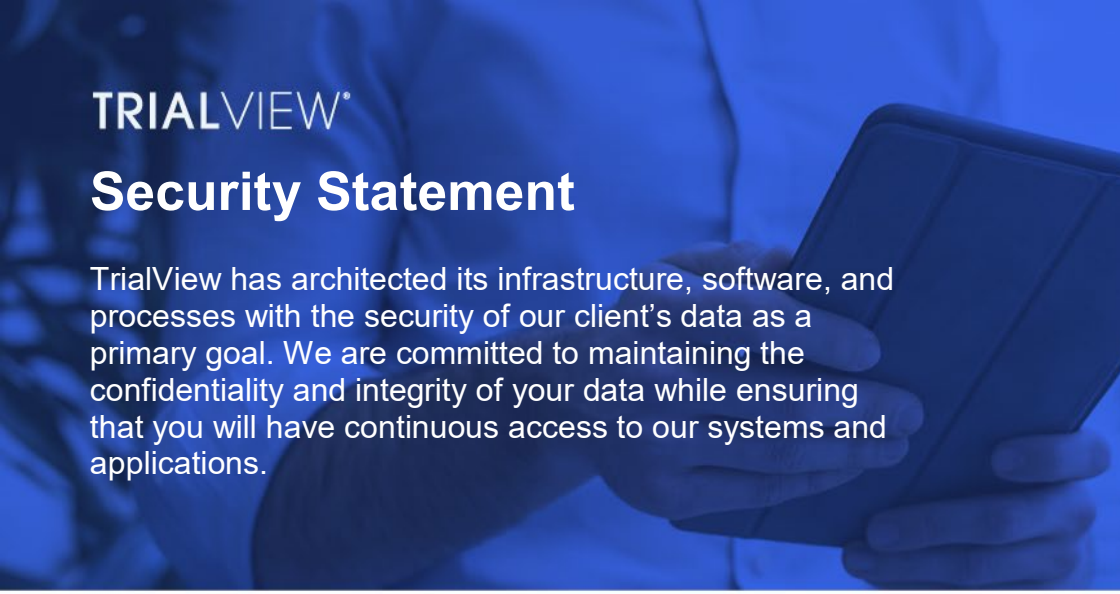
Security Whitepaper & GDPR Compliance

The information contained in this document is intended to provide transparency on TrialView's security stance and processes. We also set out our GDPR privacy and data protection policy to assist you understand how we use, protect and secure personal data.

1. TrialView Security Statement
2. Encryption and Key Management
3. GDPR Privacy Policy
4. GDPR Data Protection Policy

For further information visit trialview.com or email info@trialview.com

TRIALVIEW®



TRIALVIEW®

Security Statement

TrialView has architected its infrastructure, software, and processes with the security of our client's data as a primary goal. We are committed to maintaining the confidentiality and integrity of your data while ensuring that you will have continuous access to our systems and applications.

CONFIDENTIALITY, PRIVACY, AND ENCRYPTION

All client data in motion that traverses open, untrusted networks such as the public Internet are encrypted. All client Data at rest are encrypted;

Encryption is implemented with open source and industry-standard technologies to include Transport Layer Security (TLS), Secure Shell/Secure FTP (SSH/SFTP), and AES;

TrialView maintains separate regional environments to provide assurance of data locality. No data will be conveyed outside of the regulatory zone without express permission from the client.

When not restricted by law, we will notify data owners within twenty-four hours of the receipt of demand to release data; and

Client data are not shared with third-parties except when explicitly requested by the data owner.

AVAILABILITY

All client data are stored at Tier III+ data centers that guarantee 99.982% uptime;

We maintain active server and data resources in multiple data centers within each geographic region.

All client data are replicated to multiple data centers within a specific region;

Our application service architecture has been designed to be resilient to outage of entire data centers.

APPLICATION

The software maintains robust audit logs detailing actions undertaken by each user account;

The software implements granular access control policies that control which functions and resources a user may access;

Password policies and session timeouts are enforced;

All requests sent to the application are inspected before being forwarded to the application in order to detect anomalies and to enforce policy;

Services are powered by high availability proxies and load balancers to ensure availability and quality of service; and

Two-factor authentication can be enabled and enforced for all users on a per- case or per-environment basis.

DEVELOPMENT

Development and testing environments are maintained separately from production environments;

No data, work product, or key material are shared between production and test environments;

All development, testing, and compliance staff are located in Ireland

Releases are tested in our development and staging environments prior to installation

ENVIRONMENTAL INTEGRITY

All client data are housed at data centers that have implemented controls in alignment with ISO/IEC 27001, SOC 1/2/3 (and FedRAMP where requested)

By default, all servers restricted from sending data to the public Internet.

All servers are configured to only allow communication using those protocols and ports required for operating. All other traffic is denied.

Host-based and network-based intrusion detection systems are in place.

File integrity checks are in place to prevent the modification of application, operating system, and other trusted files.

Network and system logs are aggregated and monitored to detect anomalies.

Access to environments containing client data requires two-factor authentication.

ADMINISTRATIVE CONTROLS

Human resource process includes background checks, non-disclosure, and acceptance of policies.

TrialView has a robust information security awareness program for all staff members. This includes periodic training programs and frequent drills and tests for all employees.

TrialView maintains robust security practices including but not limited

- adherence OWASP top 10
- security coding guidelines
- use of PaaS to reduce infrastructure footprint and security perimeter
- regular penetration testing and use of 3rd party analysis tools such as Mozilla Observatory.

TRIALVIEW®

Encryption and Key Management Policy

This policy provides guidance about the use of encryption and key management. All data is encrypted in transit and at rest using strong encryption. Backup files are stored redundantly across multiple availability zones and is encrypted. TrialView is built and hosted in Microsoft Azure and leverages its encryption and key management solutions.

ENCRYPTION OF DATA AT REST

Encryption of data at rest includes information that resides in persistent storage on physical media, in any digital format.

TrialView employs following encryption

- **Disk Encryption.** TrialView uses Windows BitLocker technology and Linux DM-Crypt to protect both operating system disks and data disks with full volume encryption. Encryption keys and secrets are safeguarded with Azure Key Vault subscription.
- **Azure Storage Service Encryption.** Data at rest in Azure Blob storage and Azure file shares can be encrypted in both server-side and client-side scenarios. Azure Storage Service Encryption (SSE) automatically encrypts data before it is stored, and it automatically decrypts the data when it is retrieved. Storage Service Encryption uses 256-bit Advanced Encryption Standard (AES) encryption, which is one of the strongest block ciphers available. AES handles encryption, decryption, and key management transparently.
- **Database.** User data stored is in database encrypted by default. There are no controls to turn it on or off. Encryption at rest is implemented by using a number of security technologies, including secure key storage systems, encrypted networks, and cryptographic APIs. Encryption keys are managed by Microsoft and are rotated per Microsoft internal guidelines.

ENCRYPTION OF DATA IN TRANSIT

TLS/SSL encryption

TrialView uses the Transport Layer Security (TLS) protocol to protect data when it's traveling between the cloud services and customers. Microsoft datacenters negotiate a TLS connection with client systems that connect to Azure services. TLS provides strong authentication, message privacy, and integrity (enabling detection of message tampering, interception, and forgery), interoperability, algorithm flexibility, and ease of deployment and use.

Perfect Forward Secrecy (PFS) protects connections between customers' client systems and Microsoft cloud services by unique keys. Connections also use RSA-based 2,048-bit encryption key lengths. This combination makes it difficult for someone to intercept and access data that is in transit.

Azure Storage transactions

When TrialView interacts with Azure Storage through the Azure portal, all transactions take place over HTTPS. TrialView uses the Storage REST API over HTTPS to interact with Azure Storage. TrialView enforces the use of HTTPS when it calls the REST APIs to access objects in storage accounts by enabling the secure transfer that's required for the storage account.

KEY MANAGEMENT WITH KEY VAULT

TrialView employs Key Vault which is the Microsoft-recommended solution for managing and controlling access to encryption keys used by cloud services. Permissions to access keys can be assigned to services or to users through Azure Active Directory accounts.

With Key Vault configuration, patching, maintenance of hardware security modules (HSMs) and key management software is kept up to date. Wth Key Vault Microsoft never sees keys, and applications don't have direct access to them.

Secrets and keys are safeguarded by Azure, using industry-standard algorithms, key lengths, and hardware security modules (HSMs). The HSMs used are Federal Information Processing Standards (FIPS) 140-2 Level 2 validated.

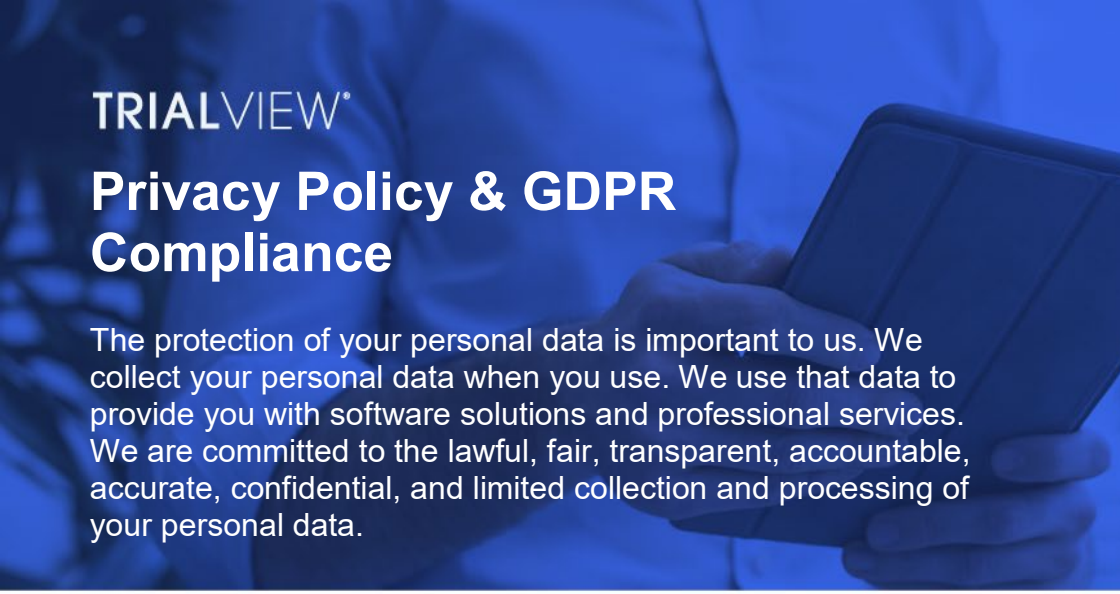
Access to a key vault requires proper authentication and authorization before a caller (user or application) can get access. Authentication establishes the identity of the caller, while authorization determines the operations that they are allowed to perform.

Authentication is done via Azure Active Directory. Authorization may be done via role-based access control (RBAC) or Key Vault access policy. RBAC is used when dealing with the management of the vaults and key vault access policy is used when attempting to access data stored in a vault.

VIDEO CONFERENCING SOLUTION

TrialView's video conferencing solution is an integrated programmable video solution built using Twillo technology, a developer platform for communications. The Twilio security framework is based on the ISO 27001 Information Security Standard. White paper available here

Twilio supports TLS 1.0, 1.1 and 1.2 to encrypt network traffic between TrialView's application and Twilio. Twilio's cloud communications platform is hosted is highly secure and reliable. It complies with leading security policies and frameworks, including SSAE 16, SOC framework, ISO 27001 and PCI DSS. All records are encrypted in transit and at rest.



TRIALVIEW®

Privacy Policy & GDPR Compliance

The protection of your personal data is important to us. We collect your personal data when you use. We use that data to provide you with software solutions and professional services. We are committed to the lawful, fair, transparent, accountable, accurate, confidential, and limited collection and processing of your personal data.

WHAT PERSONAL DATA DO WE COLLECT AND WHY?

In general, you can visit our Website without providing any identifying personal data other than the data we collect automatically. There are times, however, when we may need information from you.

To enable you to better understand what personal data we collect and how we use it we group the different kinds of data together as follows:

- Identity Data includes your name, address, email address, and, phone numbers, your professional/employment position insofar as same is relevant to accessing specific cases on the TrialView platform and for ensuring permissions, roles and access can be securely managed.

- Client Profile Data includes Client Identity Data, End User Identity Data, purchasing and payment history, customer communications and information you communicate to us about key topics and feedback you provide to us concerning our services or business;

OTHER TYPES OF PERSONAL DATA

- **Employee & Staff Data** includes Identity Data and customary personnel records concerning employees and officers of TrialView.
- **Technical Data** includes IP address, your login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices you use to access this Website;
- **Usage Data** includes information about Users's use of platform, products and services;
- **Cookies** are small files that a site transfers to your computer's hard drive through your web browser (if you allow) that enables it to recognize your browser and capture and remember certain information. A cookie cannot read data off of your hard drive or read cookie files created by other sites. Cookies may do things like allow you to navigate faster through the site, remember your preferences and passwords, and generally improve the user experience. You can turn off the ability to receive cookies by adjusting your browser settings — please note that if you do so, this may affect the functionality of the website and the information you can access through it.

WHAT WE USE DATA FOR

For access control, we're ensuring that we restrict access to data to only those who need to see it.

For account and record deletion, we align with the GDPR requirements to make sure that if you leave TrialView and close your account, or remove a specific record, your data will go away except where other laws (like taxation, audits or requests for legal hold) say we have to keep it. If you leave or ask us to delete a record, we'll work to track down data across warehouses, logs, and other storage to ensure every identifiable part of the data is deleted. So when you want something gone, we're working to make sure it's really gone.

For security, we're making sure data gets encrypted any time it could be read or intercepted by a third party.

For store and process, we're auditing and streamlining all of our data processing systems to ensure that personal data processing is limited to what helps us to deliver our products and services to you. This way the personal data is actually providing utility.

For audit and logging, we're tracking all data as it's moving, being changed, or being queried, and we're recording that access. So, if your account gets compromised, we can better tell you what somebody saw. And if you need to notify people of a breach, we can tell you what was exposed.

DATA WE COLLECT AUTOMATICALLY

Our web server logs collect the domain names and network information of visitors to our Websites automatically (such as IP address or device identifier). This information is used to measure the number of visits, average time spent on our websites, specific pages viewed, and website usage information, to meet legal or regulatory requirements, to improve the content of our sites, and to provide content to our community. This information is not collected in a way that allows identification of any of our visitors. We may, however, collect this information in a way that allows identification of our visitors by using cookies.

HOW DO WE USE COOKIES?

Cookies are small files that a site transfers to your computer's hard drive through your web browser (if you allow) that enables it to recognize your browser and capture and remember certain information. A cookie cannot read data off of your hard drive or read cookie files created by other sites. Cookies may do things like allow you to navigate faster through the site, remember your preferences and passwords, and generally improve the user experience. You can turn off the ability to receive cookies by adjusting your browser settings — please note that if you do so, this may affect the functionality of the website and the information you can access through it.

We use cookies to compile aggregate data about website traffic and interaction so that we can offer better site experiences and content in the future. We use third-party companies, such as Google Analytics, to assist us in understanding our site visitors.

THE DATA YOU PROVIDE TO US WHEN USING THE TRIALVIEW SOFTWARE

Users of the Software log into the application with their individualized credentials. These credentials are associated with your username, first name, last name, email address, and other identifying fields entered by you. We maintain robust audit logs detailing when you log into our software and the actions that you perform.

We never share personal data, cookies, audit logs, uploaded data, or any other personally identifiable information generated by or stored within our Software with a third-party without first seeking your authorization in writing. This information is referred to by TrialView as Technical Data and/or Usage Data and will also include Identity Data

If you contact our TrialView Support, then your personal data will be recorded within a support ticket to facilitate the speedy resolution of your issue. We keep this data for to track recurring issues and improve our processes and products.

WHAT SENSITIVE PERSONAL DATA DO WE COLLECT?

We do not intentionally collect any sensitive personal data. Sensitive personal data means the various categories of personal data that have been identified by applicable data privacy laws as requiring special treatment and can include data relating to ethnic origin or race, marital status, political opinions or affiliations, ideological views or activities, trade union membership, religious beliefs, physical or mental health, sexual orientation, social security information, government benefits, or administrative or criminal proceedings or records. We suggest that you do not provide sensitive personal data to us. If you do provide us with any sensitive personal data, you consent to our use of this data in the ways described in this policy.

What if you decline to provide your personal data?

Please note that if you do not provide us with personal data, we may not be able to provide you with some or all of the products or services that you have requested.

HOW DO WE SECURE YOUR PERSONAL DATA

The security of your personal data is important to us. We follow generally accepted standards to protect the personal data submitted to us, both during transmission and once we receive it. In this regard, please see our Security Policy Documentation.

For more information in relation to security please contact us.

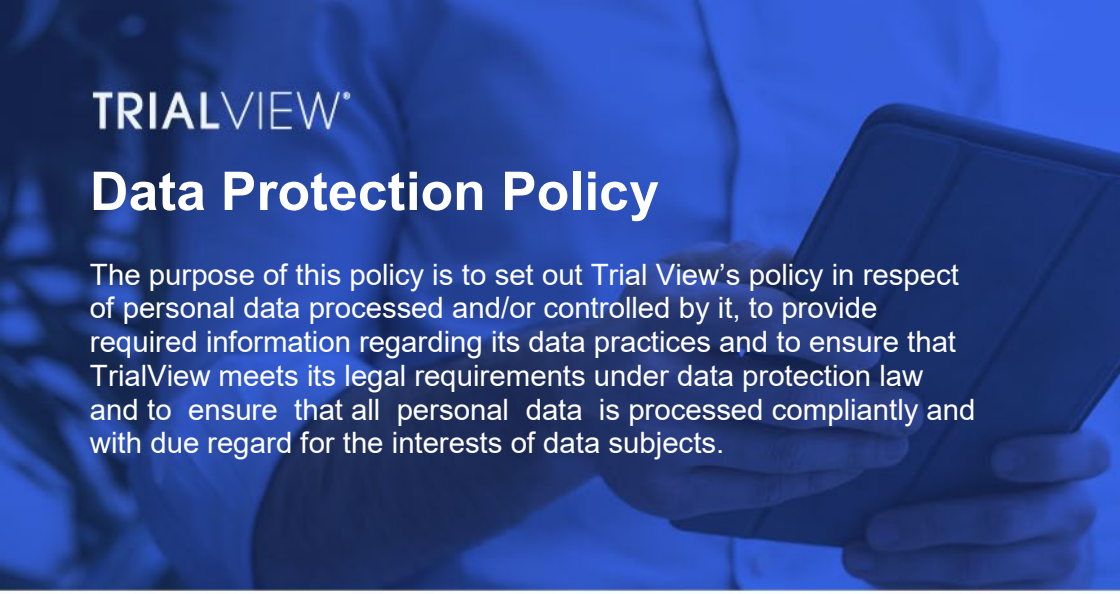
WHAT ARE YOUR RIGHTS

You have the right to send us a request to access, correct, delete, or limit the use and disclosure of your personal data in our possession and we will respond in accordance with the applicable requirements. If we cannot complete your request due to legal restrictions or because we cannot locate your data, we will let you know. These services are provided free of charge.

If after you have contacted us, you still have any unresolved issues and you live in the European Union or Switzerland, then you may contact your local Data Protection Authority for more information. The local Data Protection Authorities are a public service provided at no cost to you. For more information please visit: http://ec.europa.eu/justice/dataprotection/bodies/authorities/index_en.htm.

ENFORCEMENT

TrialView undertakes to verify compliance with its Privacy Policy not less than once per year and in connection with TrialView's annual review and internal compliance measures. TrialView will use its best commercial efforts to ensure that compliance with this Privacy Policy is maintained and that the Privacy Policy is accurate, comprehensive, and continues to conform to applicable law. We encourage CVEs to raise and discuss any issues or concerns with TrialView directly who will address and resolve such complaints regarding the use of data and noncompliance with our Privacy Policy.



TRIALVIEW®

Data Protection Policy

The purpose of this policy is to set out Trial View's policy in respect of personal data processed and/or controlled by it, to provide required information regarding its data practices and to ensure that TrialView meets its legal requirements under data protection law and to ensure that all personal data is processed compliantly and with due regard for the interests of data subjects.

DATA CONTROLLER

TrialView Limited, Suite 122, Capel Building, Mary's Abbey, Dublin 7

Email: info@trialview.com

Tel: + 353 1 440 4480

1. SCOPE OF POLICY

This policy applies to all officers, staff and contractors of TrialView.

2. PRINCIPLES

In accordance with Article 5 GDPR TrialView commits to upholding the following principles when processing personal data: -

a. to process data lawfully, fairly and in a transparent manner in relation to the data subject;

b. to collect date for specified, explicit and legitimate purposes and not to further process data in a manner that is incompatible with those purposes;

c. to process adequate and relevant personal data limited to the extent necessary for the stated purpose for which it is processed.
d. to endeavour to ensure all data is accurate and to take appropriate steps to correct any inaccuracies without delay;
e. to preserve data for no longer than is necessary for the purposes for which the personal data is processed.
f. To take appropriate measures to preserve the security and confidentiality of data processed.

3. Purpose of and Basis for Data Processing

TrialView processes personal data on behalf of clients for the purpose of providing digital trial presentation services and/or to take steps at the request of a data subject prior to being contractually engaged.

Data processing is necessary for the purposes of performing TrialView's contractual obligations to its customers in the provision of digital trial presentation services. Trial preparation and presentation services are ordinarily required for the purpose of parties efficiently and effectively managing and presenting materials in legal proceedings of some form, whether court, arbitral, statutory or other quasi-judicial proceedings. For ease of reference these various proceedings are simply referred to as proceedings in this policy.

TrialView's service contracts are ordinarily with parties' legal representatives, though occasionally they may be with institutional clients or with parties directly. Data provided by parties to proceedings and/or their representatives will be processed by Trial View and is necessary for the establishment, exercise or defence of legal claims.

4. Categories of Data Held

TrialView requires to process the following categories of documents:

- Client Files: Documents required for Court proceedings including: pleadings, orders, submissions, motions, affidavits, exhibits, witness statements, transcripts, correspondence, documents produced for discovery, intended documentary evidence, legislation, case law.
- Employee records;
- Financial Records;
- Commercial and general business documents;
- Company and corporate governance documents.

5. RECIPIENTS OF PERSONAL DATA:

TrialView may from time to time disclose personal data to:

- judicial officers and/or court officials and/or other adjudicative tribunals and/or other parties to proceedings with the express consent of the contracting party providing the relevant data;
- court reporting service providers engaged by the contracting parties with their express consent.
- TrialView's may from time to time disclose personal data to its officers & other agents or persons directly employed and/or contracted but only where necessary for the purpose of ensuring services, support and security of that data. However any such recipients will be bound by contractual obligations of confidentiality respecting the confidential and legally privileged nature of the data communicated.

6. SECURITY OF DATA PROCESSING:

TrialView will take appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

All electronically stored information is appropriately encrypted and all electronic communications of personal data are secured through SSL and/or TLS

7. TRANSMISSION OF DATA OUTSIDE THE EEA

TrialView does not allow Data to be transmitted outside of the EEA, save with the express consent and/or permission of users.

8. RETENTION OF DATA:

A. Client Files: Personal data will be retained for 90 days following the conclusion of the relevant litigation or proceedings (including the applicable time for any appeals) or such longer reasonable period as is appropriate having regard to any parties' requirements to include legal or regulatory requirements which might require TrialView to have access to the relevant personal data save where such data may need to be retained for the purpose of claims and/or legal proceedings.

B. Employee Records: 7 years from the termination of the relevant employee's employment.

C. Accounting Records: 6 years from the end of the financial year containing the latest date to which the record, information or return relate

D. VAT Records: 6 years from the day of the latest transaction to which the documents relate

9. DISPOSAL OF DATA:

See our data destruction and disposal policy

10. ACCESS TO PERSONAL DATA:

Individuals have the right to obtain from TrialView confirmation as to whether personal data concerning them is being processed, subject to any constraints of legal privilege and/or otherwise imposed by law. Individuals have a right to request access to and rectification or erasure of personal data, to request restriction of processing concerning the data subject, and to object to the

processing of data. Such requests should be made in writing to the data protection officer of the data controller using the contact details supplied below. A data subject who is dissatisfied with TrialView's response to any request, is entitled to lodge a complaint with the Data Protection Commissioner (see www.dataprotection.ie).
TrialView may require a data subject to provide appropriate validation of identity when submitting any data access request.

11. Monitoring of Staff

Staff are monitored only where strictly required to ensure

- Security protocols are being implemented
- Detection and prevention of loss of personal data (e.g. customer data)
- Detection and prevention of loss or theft of intellectual or physical business property;
- Improving employee productivity and performance;

All measures taken in this regard are assessed in advance to ensure they are necessary and proportionate to achieving these

12. Data Breaches

In the event of a personal data breach within the meaning of the GDPR, the Data Protection Commissioner will be informed without undue delay and, where feasible, within 72 hours after TrialView becomes aware of the breach, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. In the event of a personal data breach which is likely to result in a high risk to the rights and freedoms of natural persons, TrialView will notify the relevant data subject(s) without undue delay insofar as he is required to do so in accordance with the GDPR.

TrialView will observe the following protocol:

Stage 1: Identification and Classification

If a TrialView employee or contractor considers that a data security breach has occurred, this must be reported immediately to the Data Protection Officer

Stage 2: Containment and Recovery

Containment involves limiting the scope and impact of a data security breach. Appropriate action will be taken by TrialView to minimise any associated risks which may include:

- establishing who requires to be made aware of the breach;
- establishing whether there are any actions which may recover losses and limit the damage the breach can cause;

Stage 3: Risk Assessment

The Data Protection Officer will assess the potential adverse consequences for individuals, i.e. how likely they are to materialise and, if so, how serious or substantial are they likely to be, and what remedial measures are proportionate.

Stage 4: Notification of Breaches

Where applicable, the Data Protection Commissioner's Office will be notified of the breach no later than 72 hours after TrialView become aware of it.

Data Subject Notification

When a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, TrialView will initially notify its client and thereafter reserves the right to extent necessary to comply with its obligations under GDPR

to communicate directly with the affected data subject without undue delay, in a written, clear and legible format.

Stage 5: Evaluation and Response

Subsequent to a data security breach, a review of the incident by the Data Protection Officer and Management will occur to ensure that the steps taken during the incident were appropriate and to identify areas that may need to be improved.

13. Contact Details of Data Protection Officer

Frank Brooks, TrialView Limited.
Email: frankbrooks@trialview.com

TRIALVIEW®

For further information visit trialview.com
or email info@trialview.com