


Title: Data Privacy		
Document No: TOT-INT-SOP-009	Department: Information Technology	Effective Date: 13 OCT 2025
Version No: 2.0	Document Type: Standard Operating Procedure	Next Revision Date: 13 OCT 2027

1. Purpose

The purpose of this policy is to provide a framework that TOTAL Diversity Clinical Trial Management (TOTAL) adheres to for the lawful and responsible processing of Personal Data. It is intended to ensure full compliance with applicable data protection regulations, including but not limited to the General Data Protection Regulation (GDPR), EU-U.S. Data Privacy Framework (EU-U.S. DPF) and the UK Extension to the EU-U.S. DPF; and other relevant international and national privacy laws.


This policy is applicable to all TOTAL personnel, including employees, contractors, vendors, and third-party service providers—who are involved in the collection, use, storage, transmission, or disclosure of Personal Data on behalf of TOTAL.

2. Scope

This policy outlines TOTAL’s data protection measures and key principles for employees processing data.


3. Definitions

- 3.1. Applicable Data Protection Laws** Refers to all relevant legal and regulatory requirements governing personal data processing.
- 3.2. Anonymized Data** : Data that has been de-identified to the point; it is no longer considered personal. Obligations may still apply, including data security and consent for anonymization.
- 3.3. Controller** : Entity that determines the purpose and means of processing personal data.
- 3.4. Pseudonymized or Key-Coded Data** : Refers to personal data that has been processed in a way that cannot be linked to a specific individual without the use of additional, separately stored information. This additional information must be protected by appropriate technical and organizational safeguards to prevent re-identification. If the data can be reasonably linked back to an individual—such as through a code or identifier – it’s still considered Personal Data under this Policy and most applicable Data Protection laws.
- 3.5. Personal Data** : Personal Data refers to any information that directly or indirectly identifies an individual, as defined by applicable data protection laws. Examples of Personal Data may Include, but are not limited to, the following: name, date of birth, email address (professional/personal), mobile phone number (professional/personal), physical address (professional/personal), employee ID, usernames and passwords, location data.
- 3.6. Processing** : Refers to any operation or set of operations performed on personal data – whether by automated or manual means – including but not limited to collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure (by transmission or

Title: Data Privacy		
Document No: TOT-INT-SOP-009	Department: Information Technology	Effective Date: 13 OCT 2025
Version No: 2.0	Document Type: Standard Operating Procedure	Next Revision Date: 13 OCT 2027

otherwise making available), alignment, combination, restriction, erasure, or destruction.

- 3.7. Sensitive Data** : Certain types of Personal Data may be classified as sensitive or as special categories under applicable Data Protection Laws. These categories are subject to enhanced protection and additional compliance obligations due to their sensitive nature. Health and medical information, biometric identifiers, genetic data, geolocation data, information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, Details concerning an individual's sex life or sexual orientation, sensitive identifiers such as financial account numbers, social security numbers, national identification numbers, and passport details.
- 3.8. Service Provider** : TOTAL may operate as a data processor, vendor, or service provider on behalf of another entity. In such cases, TOTAL shall process, use, and disclose Personal Data strictly in accordance with the instructions provided by the data controller/customer and as permitted under applicable data protection laws.
- 4. Responsibilities**
- 4.1. All Employees** : To ensure compliance with this procedure and ensure contractual obligations are adhered with respect to records retention.
- 4.2. Data Privacy Officer (DPO)/ Chief Information Security Officer (CISO)** : The Data Privacy Officer has overall responsibility within the organization, for ensuring that appropriate security measures are taken to protect Personal Data.
The DPO shall be responsible for ensuring that appropriate measures are developed, implemented, followed, and enforced to ensure anonymization and pseudonymization.
- 4.3. Management** : Ensure adherence to applicable data protection laws and organizational privacy practices
Continuously monitor and enforce compliance with data privacy requirements
Support secure and lawful data handling within business operations
Promptly notify relevant internal teams and regulatory authorities in the event of data breach
Promote a culture of privacy awareness and information security across the organization.
- 5. Procedures**
- 5.1. Process of Anonymization**

Title: Data Privacy		
Document No: TOT-INT-SOP-009	Department: Information Technology	Effective Date: 13 OCT 2025
Version No: 2.0	Document Type: Standard Operating Procedure	Next Revision Date: 13 OCT 2027

- 5.2.**
- The principles outlined in this policy shall be applied across all customer functions/ departments involving the processing of Personal Data.
 - Only the minimum necessary Personal Data shall be collected and processed for specific, legitimate, and lawful purposes
 - Special categories of Personal Data must be protected using appropriate safeguards such as encryption or pseudonymization, whether collected directly from individuals or received from customer
 - Personal Data shall be retained only for as long as necessary to fulfill legal, regulatory, contractual, or legitimate business purposes, followed by secure and timely disposal.
 - Engagement of third parties in data collection or processing requires prior due diligence to ensure adherence to this policy and applicable regulatory requirements.
 - A Data Protection Impact Assessment (DPIA) shall be performed as needed by the customer to evaluate privacy risks prior to initiating new processes, technologies, or services involving Personal Data. Data Protection Impact Assessment (DPIA) (Privacy by Design and by Default). A DPIA is a process designed to describe the processing, assess its necessity and proportionality, and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them in agreement with customer as required.
 - Personal Data must be pseudonymized before being transferred to any third party.
 - Pseudonymization procedures must be executed solely by authorized personnel.
 - All Personal Data must be stored exclusively in organization-approved, secure storage locations; storing data on local systems is strictly prohibited.
 - Customer specific personal data shall be managed as per customer's requirements


5.3. Collection of Information

Use of the Information We Collect

- TOTAL may use the data for research studies-related information, data subjects participating in clinical trials being managed by TOTAL as a CRO or in other situations participating in clinical trials, including patients/subjects, clinical investigators or other study personnel, and other consultants, contractors, managers, and agents of the study sponsor and its corporate affiliates, business partners and third-party service providers.
- Personal Data may be used in order to carry out applicable studies and other studies-related services and/or pharmacovigilance. This may include the transfer of such personal data to the applicable study sponsor, its corporate affiliates, business partners and third-party service providers related to the study.

Security of Your Personal Information

- TOTAL shall employ reasonable security measures and technologies, such as password protection, encryption, physical locks, etc., to protect the confidentiality of your Personal Information.
- Only authorized employees have access to Personal Information. If you are an employee with such authorization, it is imperative that you take the appropriate safeguards to protect such Information. Paper and other hard copy containing Personal Information (or any other confidential information) should be secured in a locked location when not in use.
- Computers and other access points should be secured when not in use by logging out or locking. Passwords and user IDs should be guarded and not shared. When no longer necessary for business purposes, paper and hard copies should be immediately destroyed using paper shredders or similar devices. Do not leave copies in unsecured locations waiting to be shredded or otherwise destroyed. Do not make or distribute unauthorized copies of documents or other tangible medium containing personal

Title: Data Privacy		
Document No: TOT-INT-SOP-009	Department: Information Technology	Effective Date: 13 OCT 2025
Version No: 2.0	Document Type: Standard Operating Procedure	Next Revision Date: 13 OCT 2027

data. Electronic files containing Personal Information should only be stored on secure computers and not copied or otherwise shared with unauthorized individuals within or outside of Company.


- The Company shall make reasonable efforts to secure Personal Information stored or transmitted electronically secure from hackers or other persons who are not authorized to access such Information.
- Compliance with this Privacy Policy is important to the Company. Any violation or potential violation of this Policy should be reported Data Privacy Officer on dataprotection@totalcro.com. The failure by any employee to follow these privacy policies may result in discipline up to and including separation of the employment.
- Additionally, it is important to note that TOTAL may be required to disclose the personal information of individuals, including certain personally identifiable information, in response to a lawful request by public authorities or under any applicable law, including to meet national security or law enforcement requirements
- Data Subjects may initiate a request relating to their data, and, under certain circumstances, may invoke binding arbitration. TOTAL shall use commercially reasonable efforts to respond to individual requests within forty-five (45) days of receipt of such request and proper identity verification. All requests in this regard should be submitted via email to dataprotection@totalcro.com. We use your personal information as necessary or appropriate to:
 - Enforce the terms and conditions that govern our Services.
 - Protect our rights, privacy, safety or property, and/or that of you or others.
 - Protect, investigate and deter against fraudulent, harmful, unauthorized, unethical or illegal activity

5.4. How We Share Your Personal Information

TOTAL does not share the personal information provided with other organizations. In cases where TOTAL may share data with agents, third-parties, or partners approved by our customers and as required by contract. TOTAL shall not disclose any data to third parties without explicit approval from customer. In cases where TOTAL contracts with a third-party, then TOTAL shall obtain assurances that they shall safeguard Personal Data and study data in a manner consistent with this Policy.

Furthermore, when transferring personal information to a third party acting as an agent, TOTAL shall:

- Transfer such data only for limited and specified purposes
- Ascertain that the agent is obligated to provide at least the same level of privacy protection as is required by the EU-U.S. Data Privacy Framework (EU-U.S. DPF) and the UK Extension to the EU-U.S. DPF;
- Take reasonable and appropriate steps to ensure that the agent effectively processes the personal information transferred in a manner consistent with the organization's obligations under the principles;
 - Require the agent to notify the organization if it decides that it can no longer meet its obligation to provide the same level of protection as is required by the principles;
 - Upon notice, including under (iv), take reasonable and appropriate steps to stop and remediate unauthorized processing; and
 - Provide a summary or a representative copy of the relevant privacy provisions of our contract with that agent to the Department of Commerce or Federal Trade Commission upon verified request as applicable.
 - Such third-party agents are restricted from using this data in any way other than providing services for or on behalf of TOTAL. We disclose personal information to third parties under the following circumstances.
 - **Service Providers:** TOTAL may employ third party companies and individuals to administer and provide the Services on our behalf (such as training, shipping, customer support, hosting, email delivery, and database management services). These third parties may use your information only

Title: Data Privacy		
Document No: TOT-INT-SOP-009	Department: Information Technology	Effective Date: 13 OCT 2025
Version No: 2.0	Document Type: Standard Operating Procedure	Next Revision Date: 13 OCT 2027

as directed by TOTAL and in a manner consistent with this Privacy Policy, and are prohibited from using or disclosing your information for any other purpose


- **Compliance with Laws and Law Enforcement; Protection and Safety:** TOTAL may disclose information about you to government or law enforcement officials or private parties as required by law, and disclose and use such information as we believe necessary or appropriate to:
 - a) Comply with applicable laws and lawful requests and legal process, such as to respond to subpoenas or requests from government authorities.
 - b) Enforce the terms and conditions that govern our Services.
 - c) Protect our rights, privacy, safety or property, and/or that of you or others.
 - d) Protect, investigate, and deter against fraudulent, harmful, unauthorized, unethical, or illegal activity.

5.5. A Data Protection Impact Assessment (DPIA) shall be performed as needed by the customer to evaluate privacy risks prior to initiating new processes, technologies, or services involving Personal Data. Data Protection Impact Assessment (DPIA) (Privacy By Design and by Default). A DPIA is a process designed to describe the processing, assess its necessity and proportionality, and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them in agreement with customer, if required.

5.6. Compliance

- In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF, TOTAL complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF) and the UK Extension to the EU-U.S. DPF, as set forth by the U.S. Department of Commerce.
- TOTAL has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of personal data received from the European Union and the United Kingdom in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF. If there is any conflict between the terms in this privacy policy and the EU-U.S. DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework (DPF) program, please visit <https://www.dataprivacyframework.gov/>
- TOTAL commits to resolve DPF Principles-related complaints about our collection and use of your personal information. EU and UK individuals with inquiries or complaints regarding our handling of personal data received in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF, should first contact TOTAL at dataprotection@totalcro.com
- In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF, TOTAL commits to cooperate and comply respectively with the advice of the panel established by the EU data protection authorities (DPAs) and the UK Information Commissioner's Office (ICO) with regard to unresolved complaints concerning our handling of personal data received in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF
- By self-certifying with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF, TOTAL is subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC).

5.7. Governance, Management, Personal Data Breach Accountability


Title: Data Privacy		
Document No: TOT-INT-SOP-009	Department: Information Technology	Effective Date: 13 OCT 2025
Version No: 2.0	Document Type: Standard Operating Procedure	Next Revision Date: 13 OCT 2027

- TOTAL shall appoint a Data Privacy Officer (DPO) to oversee the development, implementation, and enforcement of policies and procedures related to Personal Data. The DPO shall be responsible for
 - Ensuring alignment of company practices with applicable Data Protection Laws
 - Coordinating with relevant teams to maintain and monitor data security controls
 - Conducting privacy and data protection due diligence for third parties, including vendors, as required by customer/sponsor or regulatory obligations
 - DPO shall access compliance to include assurance mechanisms, such as monitoring and auditing/ review of the data privacy controls, including Privacy by Design, Privacy Impact Assessments, and record retention as agreed with the customer as applicable
- A personal data breach is a security breach that can lead to accidental or deliberate loss, destruction, corruption, unauthorized disclosure, or alteration of personal data that can cause material or non-material damage to individuals.
- A Personal Data Breach response plan is documented, maintained in current order and ready to be implemented, as necessary.
- Where a known or suspected breach is discovered, employees shall report to the DPO. The incident notification can be sent over an e-mail to dataprotection@totalcro.com immediately to no later than one (01) business day. This notification clearly indicates the Personal Data Breach issue and provides as much known detail as possible without delay for follow-up and investigation.
- Alerts from the IT team or suppliers or any other stakeholders shall be expected to be communicated directly to the DPO. Upon receiving an alert DPO shall as applicable
 - Verify the facts by having a direct conversation with reporting personnel or suppliers as applicable
 - Determine the need to address, and as appropriate action, any time-critical notification to Management or communications to affected data subjects
 - The DPO shall maintain an oversight on the response process ensuring that the response structure is an appropriate fit to the case being managed and that the response is compliant with applicable regulations
 - Upon completion of each Personal Data Breach case, DPO shall ensure an appropriate review is undertaken with relevant parties as applicable to check that all appropriate documentation has been captured in the case management system; identify key lessons; determine whether technological or organizational changes are appropriate to prevent future breaches; determine recommended changes to plans and processes; and determine whether any further awareness or training sessions are appropriate.
 - Following parties may be notified as applicable immediately no later than thirty (30) business days of becoming aware of any breach or as agreed with the customer:
 - Individuals (Data Subjects) affected by the breach.
 - Relevant Supervisory Authority as applicable
 - Other bodies such as regulatory bodies, investor /financer/ promoter group, legal advisers as applicable
 - Customers as applicable.

TOTAL may share study data with agents, third-parties, or partners approved by customers and as required by contract. Therefore, TOTAL is liable for the onward transfers to these approved agents, third-parties, or partners.

5.8. Transparency

- TOTAL shall ensure that appropriate notice is provided for any new data collection, use, or processing activity, supported by a privacy assessment where applicable.

Title: Data Privacy		
Document No: TOT-INT-SOP-009	Department: Information Technology	Effective Date: 13 OCT 2025
Version No: 2.0	Document Type: Standard Operating Procedure	Next Revision Date: 13 OCT 2027

- If notice is not provided at the time of collection, the Personal Data may be deemed unlawfully obtained and subject to deletion:
 - A valid notice must be clearly disclosed.
 - The types of Personal Data collected or received
 - The source of Personal Data
 - The recipients or categories of recipients of the data
 - The purposes and legal bases for processing
 - Any cross-border data transfers
 - The data subject's rights, including the right to lodge a complaint
 - Data retention periods
 - Security measures in place to protect the data
 - Contact information for further inquiries

5.9. Acquisition and Disclosure of Personal Information


- Employees must ensure appropriate notice is provided when collecting or receiving Personal Data from third parties, and the same applies when disclosing such data to external parties
- TOTAL shall ensure that third parties uphold all applicable data protection obligations in line with the company's responsibilities.

5.10. Data Access Control and Integrity Assurance

- TOTAL ensures individuals have reasonable access to their Personal Information and may request corrections, amendments, or deletions if the data is inaccurate or incomplete
- TOTAL takes appropriate measures to protect Personal Information from loss, misuse, unauthorized access, disclosure, alteration, or destruction.
- Data must be relevant, accurate, complete, and current for its intended purpose, and TOTAL applies reasonable safeguards to maintain its integrity and security.
- TOTAL should inform individuals about the choices and means organization offers individuals for limiting the use and disclosure of their personal data.
- TOTAL offers individuals the opportunity to choose (opt out) whether their personal information is (i) to be disclosed to a third party or (ii) to be used for a purpose that is materially different from the purpose(s) for which it was originally collected or subsequently authorized by the individuals. Individuals must be provided with clear, conspicuous, and readily available mechanisms to exercise choice

5.11. Built-In Privacy Controls and Safeguards

- TOTAL integrates data protection principles into the design and default settings of all systems, processes, and solutions involving the processing of Personal Data. TOTAL has implemented certain security measures, including requirements on data protection by design and default, which we are required to comply. Privacy by design and by default indicates a process or practice for data protection principles to be integrated into and applied as a default setting in the processing use, and handling of Personal Data and in related business practices from the design state throughout launch of the engagement of project services, data use or solutions.
- This proactive approach ensures compliance from the initial stages of any project or service engagement through its full lifecycle. Key principles include:

Title: Data Privacy		
Document No: TOT-INT-SOP-009	Department: Information Technology	Effective Date: 13 OCT 2025
Version No: 2.0	Document Type: Standard Operating Procedure	Next Revision Date: 13 OCT 2027

- Limiting the collection, use, and disclosure of Personal Data to what is strictly necessary for its intended purpose
- Restricting access to Personal Data to authorized personnel only
- Maintaining transparency with individuals regarding how their data is used
- Ensuring fair and lawful processing of Personal Data
- Retaining Personal Data only for as long as necessary to fulfill its purpose
- Applying appropriate technical and organizational safeguards to protect Personal Data from unauthorized access, loss, or breach
-

5.12. Storage Limitation/Records Management

- TOTAL intends to keep Personal Data in its control accurate and up to date and shall retain Personal Data only as long as it is necessary to carry out the purposes or as agreed with the customer as applicable.
- TOTAL shall maintain reasonable administrative, technical, and physical safeguards to protect Personal Data against accidental or unlawful destruction, or loss, alteration, unauthorized disclosure or access, erasure, modification, transfer/portability in line with applicable law/ adequate level of protection for the Personal Data and that appropriate security measures are in place as agreed with the customer as applicable
- TOTAL shall delete personal data when it's no longer necessary. This shall depend on the purposes for holding the data and periodically reviewing the data, erased or anonymized when we no longer needed discussion with the Management team or as agreed with the customer as applicable.

6. References


- 6.1 General Data Protection Regulation (GDPR) – Regulation (EU) 2016/679
- 6.2 The California Consumer Privacy Act of 2018 (CCPA)
- 6.3 The Digital Personal Data Protection Act, 2023
- 6.4 The Health Insurance Portability and Accountability Act (HIPPA)
- 6.5 [Data Privacy Framework](#)
- 6.6 TOT-CLO-SOP-005 _Control of Records Retention and Restoration Procedure

7. Annexure

Nil

8. Revision History

Version Number	Change Description	Effective Date
0.0	<ul style="list-style-type: none"> • Initial release 	07 MAY 2025

Title: Data Privacy		
Document No: TOT-INT-SOP-009	Department: Information Technology	Effective Date: 13 OCT 2025
Version No: 2.0	Document Type: Standard Operating Procedure	Next Revision Date: 13 OCT 2027

2.0	<ul style="list-style-type: none"> Document updated as per TOT-ADM-SOP-001_ Writing and Revising Procedural Documents. OneQMS does not have a functionality to publish version 0.0 hence, the documents were published as 1.0 instead of 0.0. Hence, this version is captured as 2.0 instead of 1.0 Title updated to Data Privacy. Updated the policy to responsibilities for management team in section 4.2 Policy has been updated to include requirements from EU-U.S. Data Privacy Framework (EU-U.S. DPF) and the UK Extension to the EU-U.S. DPF Section 5.3 on collection and section 5.4 on how we share personal information added. This policy has been updated to add information around individual choices. Section 5.6 on Compliance added Reference section 6 updated. 	13 OCT 2025
-----	--	-------------