

Triton Showers  
Data Protection Policy

---

## Table of contents

<b>1. Introduction</b> .....	2
<b>2. Scope</b> .....	2
<b>3. Definitions</b> .....	3
<b>4. Policy</b> .....	4
<b>4.1 Data Protection Principles</b> .....	4
<b>4.2 Data Collection</b> .....	5
<b>4.3 Data Subject Consent</b> .....	5
<b>4.4 Data Use</b> .....	6
<b>4.4.1 Data Processing</b> .....	6
<b>4.4.2 Special Categories of Data</b> .....	7
<b>4.4.3 Data Quality</b> .....	7
<b>4.4.4 Digital Marketing</b> .....	7
<b>4.5 Data Retention</b> .....	8
<b>4.6 Data Protection</b> .....	8
<b>4.7 Data Subject Requests</b> .....	8
<b>4.8 Law Enforcement Requests &amp; Disclosures</b> .....	10
<b>4.9 Data Protection Training</b> .....	10
<b>4.10 Data Transfers</b> .....	10
<b>4.10.1 Transfers between Norcros Businesses Entities</b> .....	11
<b>4.10.2 International Transfers</b> .....	11
<b>4.10.3 Transfers to Third Parties</b> .....	11
<b>4.11 Complaints Handling</b> .....	11
<b>4.12 Breach Reporting</b> .....	12
<b>5. Further Data Protection Policies and Procedures</b> .....	12

## **1. Introduction**

Triton Showers is committed to conducting its business in accordance with all applicable Data Protection laws and regulations and in line with the highest standards of ethical conduct.

This policy sets forth the expected behaviours of Triton employees and third parties in relation to the collection, use, retention, transfer, disclosure, and destruction of any Personal Data belonging to a Triton Contact (i.e., the Data Subject).

Personal Data is any information (including opinions and intentions) which relates to an identified or Identifiable Natural Person. Personal Data is subject to certain legal safeguards and other regulations, which impose restrictions on how organisations may process Personal Data. An organisation that manages Personal Data and makes decisions about its use is known as a Data Controller. Triton, as a Data Controller, is responsible for ensuring compliance with the Data Protection requirements outlined in this policy. Non-compliance may expose Triton to complaints, regulatory action, fines and/or reputational damage.

Triton Showers leadership is fully committed to ensuring continued and effective implementation of this policy and expects all Triton employees and third parties to share in this commitment. Any breach of this policy will be taken seriously and may result in disciplinary action or business sanction.

## **2. Scope**

This policy applies to Triton Showers and refers to all data subjects (employees, job candidates, customers, suppliers etc.) who provide any amount of information to us.

This policy applies to all Processing of Personal Data in electronic form (including electronic mail and documents created with word processing software) or where it is held in manual files structured in a way that allows ready access to information about individuals.

This policy establishes a baseline standard for the Processing and protection of Personal Data by Triton Showers. Where national law imposes a requirement, which is stricter than imposed by this policy, the requirements in national law must be followed. Furthermore, where national law imposes a requirement that is not addressed in this policy, the relevant national law must be adhered to.

If there are conflicting requirements in this policy and national law, please consult with Norcros Group Counsel, Richard Collins – [richardcollins@norcros.com](mailto:richardcollins@norcros.com)

### 3. Definitions

In this policy document there are key words and phrases. For clarity, please note the meanings as follows:

<b>Contact</b>	The potential or actual Data Subject.
<b>Data Controller</b>	A 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.
<b>Data Processors</b>	A natural or legal person, public authority, agency, or other body which Processes Personal Data on behalf of a Data Controller.
<b>Data Protection</b>	The process of safeguarding Personal Data from unauthorised or unlawful disclosure, access, alteration, Processing, transfer, or destruction.
<b>Data Subject</b>	The identified or Identifiable Natural Person to which the data refers.
<b>Identifiable Natural Person</b>	Anyone identifiable, directly, or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
<b>Personal Data</b>	Any information (including opinions and intentions) which relates to an identified or Identifiable Natural Person.
<b>Process, Processed, Processing</b>	Any operation or set of operations performed on Personal Data or on sets of Personal Data, whether by automated means or not. Operations performed may include 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.
<b>Special Categories</b>	<p>The Processing relates to Personal Data which has already been made public by the Data Subject.</p> <p>The Processing is necessary for the establishment, exercise, or defence of legal claims.</p> <p>The Processing is specifically authorised or required by law.</p> <p>The Processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving consent.</p> <p>Further conditions, including limitations, based upon national law related to the Processing of genetic data, biometric data or data concerning health</p>

## 4. Policy

### 4.1 Data Protection Principles

Triton has adopted the following principles to govern its collection, use, retention, transfer, disclosure, and destruction of Personal Data:

<b>Principle 1: Lawfulness, Fairness and Transparency</b>	Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. This means we must tell the Data Subject what Processing will occur (transparency), the Processing must match the description given to the Data Subject (fairness), and it must be for one of the purposes specified in the applicable Data Protection regulation (lawfulness).
<b>Principle 2: Purpose Limitation</b>	Personal Data shall be collected for specified, explicit and legitimate purposes and not further Processed in a manner incompatible with those purposes. This means we must specify what the Personal Data collected will be used for and limit the Processing of that Personal Data to only what is necessary to meet the specified purpose.
<b>Principle 3: Data Minimisation</b>	Personal Data shall be adequate, relevant, and limited to what is reasonably necessary in relation to the purposes for which they are Processed. This means we must not store any Personal Data beyond what is required.
<b>Principle 4: Accuracy</b>	Personal Data shall be accurate and, kept up to date. This means we must have in place processes for identifying and addressing out-of-date, incorrect, and redundant Personal Data.
<b>Principle 5: Storage Limitation</b>	Personal Data shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data is Processed. This means we must, wherever reasonably possible, store Personal Data in a way that limits or prevents identification of the Data Subject.
<b>Principle 6: Integrity &amp; Confidentiality</b>	Personal Data shall be Processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful Processing, and against accidental loss, destruction, or damage. We must use appropriate technical and organisational measures to ensure the integrity

	and confidentiality of Personal Data is maintained always.
<b>Principle 7: Accountability</b>	The Data Controller shall be responsible for and must be able to demonstrate compliance. This means we must demonstrate the six Data Protection Principles (outlined above) are met for all Personal Data for which we are responsible.

#### 4.2 Data Collection

Personal Data will only be collected from the Data Subject unless one of the following apply

- The nature of the business purpose necessitates collection of the Personal Data from other persons or bodies.
- The collection must be carried out under emergency circumstances to protect the vital interests of the Data Subject or to prevent serious loss or injury to another person.

If Personal Data is collected from someone other than the Data Subject, the Data Subject must be informed of the collection unless one of the following apply:

- The Data Subject has received the required information by other means.
- The information must remain confidential due to a secrecy or confidentiality obligation.
- A national law expressly provides for the collection, Processing, or transfer of the Personal Data.

Where it has been determined the Data Subject should be notified, notification must occur promptly, but in no case later than:

- One calendar month from the first collection or recording of the Personal Data
- At the time of first communication if used for communication with the Data Subject
- At the time of disclosure if disclosed to another recipient.

#### 4.3 Data Subject Consent

Triton Showers will obtain Personal Data only by lawful and fair means and, where appropriate with the knowledge and Consent of the individual concerned. Where a need exists to request and receive the Consent of an individual prior to the collection, use or disclosure of their Personal Data, Triton is committed to seeking such Consent and each business will be responsible for:

- Determining what disclosures should be made to obtain valid Consent.
- Ensuring the request for consent is presented in a manner which is clearly distinguishable from any other matters, is made in an intelligible and easily accessible form, and uses clear and plain language.

- Ensuring the Consent is freely given (i.e., is not based on a contract conditional to the Processing of Personal Data unnecessary for the performance of that contract).
- Documenting the date, method and content of the disclosures made, as well as the validity, scope, and volition of the Consents given.
- Providing a simple method for a Data Subject to withdraw their Consent at any time.

#### **4.4 Data Use**

##### **4.4.1 Data Processing**

Triton uses the Personal Data of its Contacts for the following broad purposes:

- The general running and business administration of the Businesses.
- To provide goods and services to customers.
- The ongoing administration and management of customer services.

Triton will Process Personal Data in accordance with all applicable laws and contractual obligations. More specifically, Personal Data will not be processed unless at least one of the following requirements are met:

- The Data Subject has given Consent to the Processing of their Personal Data for one or more specific purposes.
- Processing is necessary for the performance of a contract to which the Data Subject is party or to take steps at the request of the Data Subject prior to entering a contract.
- Processing is necessary for compliance with a legal obligation to which the Data Controller is subject.
- Processing is necessary to protect the vital interests of the Data Subject or of another natural person.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller.
- Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a third party (except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject).

In any circumstance where consent has not been gained for the specific Processing in question, Triton will address the following additional conditions to determine the fairness and transparency of any Processing beyond the original purpose for which the Personal Data was collected:

- Any link between the purpose for which the Personal Data was collected and the reasons for intended further Processing.
- The context in which the Personal Data has been collected, regarding the relationship between Data Subject and the Data Controller.
- The nature of the Personal Data, whether Special Categories (see 4.4.2) of Data are being Processed, or whether Personal Data related to criminal convictions and offences are being Processed.
- The possible consequences of the intended further Processing for the Data Subject.
- The existence of appropriate safeguards pertaining to further Processing, which may include encryption, anonymisation or pseudonymisation.

#### **4.4.2 Special Categories of Data**

Triton will only Process Special Categories of Data (also known as sensitive data) where the Data Subject expressly consents to such Processing or where one of the following conditions apply:

- The Processing relates to Personal Data which has already been made public by the Data Subject.
- The Processing is necessary for the establishment, exercise, or defence of legal claims.
- The Processing is specifically authorised or required by law.
- The Processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving consent.
- Further conditions, including limitations, based upon national law related to the Processing of genetic data, biometric data or data concerning health.

#### **4.4.3 Data Quality**

Triton will adopt all necessary measures to ensure the Personal Data it collects, and Processes is complete and accurate in the first instance and is updated to reflect the current situation of the Data Subject. This will include:

- Correcting Personal Data known to be incorrect, inaccurate, incomplete, ambiguous, misleading, or outdated, even if the Data Subject does not request rectification.
- Keeping Personal Data only for the period necessary to satisfy the permitted uses or applicable statutory retention period.
- The removal of Personal Data if in violation of any of the Data Protection principles or if the Personal Data is no longer required.
- Restriction, rather than deletion of Personal Data, as far as:
  - a law prohibits erasure.
  - erasure would impair legitimate interests of the Data Subject.
  - the Data Subject disputes their Personal Data is correct, and it cannot be clearly ascertained whether their information is correct or incorrect.

#### **4.4.4 Digital Marketing**

Triton will not send promotional or direct marketing material to a Contact through digital channels such as mobile phones, email, and the Internet, without first obtaining their Consent.

Where Personal Data Processing is approved for digital marketing purposes, the Data Subject must be informed at the point of first contact they have the right to object, at any stage, to having their data Processed for such purposes. If the Data Subject puts forward an objection, digital marketing related Processing of their Personal Data must cease immediately, and their details should be kept on a suppression list with a record of their opt-out decision, rather than being completely deleted.

It should be noted where digital marketing is conducted in a 'business to business' context, there is no legal requirement to obtain an indication of Consent to carry out digital marketing to individuals if they are given the opportunity to opt-out.

#### **4.5 Data Retention**

To ensure fair processing, Personal Data will not be retained for longer than necessary in relation to the purposes for which it was originally collected, or for which it was further Processed.

Data retention periods are set out in the Data Retention Policy which ensures:

- There is a clearly identified retention period for each document or record type.
- Procedures exist which identify and eliminate as soon as possible documents of only short-term interest (i.e., they are not records); and
- All Personal Data is deleted or destroyed as soon as possible where it has been confirmed there is no longer a need to retain it.

#### **4.6 Data Protection**

Triton will adopt physical, technical, and organisational measures to ensure the security of Personal Data. This includes the prevention of loss or damage, unauthorised alteration, access or Processing, and other risks to which it may be exposed by virtue of human action or the physical or natural environment.

The minimum set of security measures to be adopted by Triton is provided in the 'Information Security Standard'. A summary of the Personal Data related security measures is provided below:

- Prevent unauthorised persons from gaining access to data processing systems in which Personal Data are Processed.
- Prevent persons entitled to use a data processing system from accessing Personal Data beyond their needs and authorisations.
- Ensure Personal Data during electronic transmission/transport cannot be read, copied, modified, or removed without authorisation.
- Ensure access logs, or processes are in place to establish whether, and by whom, the Personal Data was entered, modified on or removed from a data processing system.
- Ensure where Processing is conducted by a Data Processor, the data can be Processed only in accordance with the instructions of the Data Controller.
- Ensure Personal Data is protected against undesired destruction or loss.
- Ensure Personal Data collected for different purposes can and is processed separately.
- Ensure Personal Data is not kept longer than necessary.

#### **4.7 Data Subject Requests**

Triton will establish a process to enable and facilitate the exercise of Data Subject rights related to:

- Information access.
- Objection to Processing.
- Objection to automated decision-making and profiling.
- Restriction of Processing.
- Data portability.
- Data rectification.
- Data erasure.

Any request made by an individual relating to any of the rights listed above will be considered in accordance with all applicable Data Protection laws and regulations. No administration fee will be charged for considering and/or complying with such a request unless the request is deemed to be unnecessary or excessive in nature.

Data Subjects are entitled to obtain, based upon a request made in writing to the Business concerned, and upon successful verification of their identity, the following information about their own Personal Data:

- The purposes of the collection, Processing, use and storage of their Personal Data.
- The source(s) of the Personal Data if it was not obtained from the Data Subject.
- The categories of Personal Data stored for the Data Subject.
- The recipients or categories of recipients to whom the Personal Data has been or may be transmitted, along with the location of those recipients.
- The envisaged period of storage for the Personal Data or the rationale for determining the storage period.
- The use of any automated decision-making, including Profiling.
- The right of the Data subject to:
  - object to Processing of their Personal Data.
  - lodge a complaint with the Data Protection Authority.
  - request rectification or erasure of their Personal Data.
  - request restriction of Processing of their Personal Data.

All requests received for access to, or rectification of Personal Data must be logged as received. A response to each request will be provided within 30 days of the receipt of the written request from the Data Subject. Appropriate verification must confirm the requestor is the Data Subject or their authorised legal representative. Data Subjects shall have the right to require the Business to correct or supplement erroneous, misleading, outdated, or incomplete Personal Data.

If Triton cannot respond fully to the request within 30 days, it shall nevertheless provide the following information to the Data Subject, or their authorised legal representative within the specified time:

- An acknowledgement of receipt of the request.
- Any information located to date.
- Details of any requested information or modifications which will not be provided to the Data Subject, the reason(s) for the refusal, and any procedures available for appealing the decision.
- An estimated date by which any remaining responses will be provided.
- An estimate of any costs to be paid by the Data Subject (e.g., where the request is excessive in nature).
- The name and contact information of the individual who the Data Subject should contact for follow up.

In situations where providing the information requested by a Data Subject would disclose Personal Data about another individual information must be redacted or withheld as may be necessary or appropriate to protect that person's rights.

#### **4.8 Law Enforcement Requests & Disclosures**

In certain circumstances, it is permitted Personal Data be shared without the knowledge or Consent of a Data Subject. Examples include the following purposes:

- The prevention or detection of crime.
- The apprehension or prosecution of offenders.
- The assessment or collection of a tax or duty.
- By the order of a court or by any rule of law.

If Triton Processes Personal Data for one of these purposes, then it may apply an exception to the Processing rules outlined in this policy but only to the extent not doing so would be likely to prejudice the case in question.

If Triton receives a request from a court or any regulatory or law enforcement authority for information relating to a Contact, the Group General Counsel will be immediately notified and will provide comprehensive guidance and assistance.

#### **4.9 Data Protection Training**

Employees with access to Personal Data will have their responsibilities under this policy outlined to them as part of their induction training. In addition, Triton will provide regular Data Protection training and procedural guidance for their staff covering the following elements:

- The Data Protection Principles set forth in Section 4.1 above.
- Each Employee's duty to use and permit the use of Personal Data only by authorised persons and for authorised purposes.
- The need for, and proper use of, the forms and procedures adopted to implement this policy.
- The correct use of passwords, security tokens and other access mechanisms.
- The importance of limiting access to Personal Data, such as by using password protected screen savers and logging out when systems are not in use.
- Securely storing manual files, print outs and electronic storage media.
- The need to obtain appropriate authorisation and utilise appropriate safeguards for all transfers of Personal Data outside of the internal network and physical office premises.
- Proper disposal of Personal Data by using confidential waste secure shredding facilities.
- Any special risks associated with departmental activities or duties.

#### **4.10 Data Transfers**

Triton may only transfer Personal Data where one of the following conditions apply:

- The Data Subject has given Consent to the proposed transfer.

- The transfer is necessary for the performance of a contract with the Data Subject.
- The transfer is necessary for the implementation of pre-contractual measures taken in response to the Data Subject's request.
- The transfer is necessary for the conclusion or performance of a contract concluded with a Third Party in the interest of the Data Subject.
- The transfer is legally required on important public interest grounds.
- The transfer is necessary for the establishment, exercise, or defence of legal claims.
- The transfer is necessary to protect the vital interests of the Data Subject.

#### **4.10.1 Transfers between Norcros Businesses Entities**

For Norcros to carry out its operations effectively across its various businesses there may be occasions when it is necessary to transfer personal data from one business to another. In these circumstances the business sending the data remains responsible for ensuring protection of that data.

#### **4.10.2 International Transfers**

When transferring Personal Data to any entity located in a Third Country, Triton will follow the established "procedure for the international transfer of personal data" to ensure such transfers meet all legislative requirements.

#### **4.10.3 Transfers to Third Parties**

Triton will only transfer Personal Data to, or allow access by, Third Parties when it is assured the information will be Processed legitimately and protected appropriately by the recipient. Where Third Party Processing takes place, Triton will first identify if, under applicable law, the Third Party is considered a Data Controller, or a Data Processor of the Personal Data being transferred.

Where the Third Party is deemed to be a Data Controller, Triton will enter into an appropriate agreement with the Controller to clarify each party's responsibilities in respect to the Personal Data transferred.

Where the Third Party is deemed to be a Data Processor, the Business will enter into an adequate Processing agreement with the Data Processor. The agreement must require the Data Processor to protect the Personal Data from further disclosure and to only Process Personal Data in compliance with our instructions. In addition, the agreement will require the Data Processor to implement appropriate technical and organisational measures to protect the Personal Data as well as procedures for providing notification of Personal Data Breaches. Triton has a 'Standard Data Processing Agreement' document for use as a baseline template.

#### **4.11 Complaints Handling**

Triton will have a process for dealing promptly with Data Subjects with a complaint about the Processing of their Personal Data. All such complaints should put forward in writing to the relevant Triton Data Champion who will initiate an investigation of the complaint to the appropriate extent based on the merits of the specific case. The Triton Data Champion will inform the Data Subject of the progress and the outcome of the complaint within a reasonable period.

If the issue cannot be resolved through consultation between the Data Subject and the Triton Data Champion, then the Data Subject may, at their option, seek redress through mediation, binding

arbitration, litigation, or via complaint to the Data Protection Authority within the applicable jurisdiction.

#### **4.12 Breach Reporting**

Triton has established a data breach response plan (“plan”) setting out procedures and clear lines of authority for the management and staff of Triton. The plan is implemented if Triton experiences a data breach (or suspects a data breach has occurred), and is intended to enable the business to contain, assess and respond to data breaches in a timely fashion, to help mitigate potential harm to affected individuals. It sets out contact details for the appropriate Triton and Norcros people in the event of a data breach, clarifies roles and responsibilities, and documents processes to assist Triton to respond to a data breach.

#### **5. Further Data Protection Policies and Procedures**

To give effect to this overarching policy Triton will maintain the following policies and procedures which can be obtained from the Triton Data Champion:

- Document Retention
- Information Classification
- International Transfer of Personal Data
- Data Subject Access Request Procedure
- Data Breach Response Procedure
- Data Privacy Impact Assessment Procedure