SOTRAVIC
water · environment · energy

bakertilly

Data Protection Policy

Sotravic Limitee

The aim of the Data Protection Policy is to provide a concise and practical document that can be used at Sotravic Limitee including its subsidiaries and affiliated entities ("the Group"). The Data Protection Policy provides the foundation of the data privacy practices regarding the processing of personal and sensitive data.

Date Policy Prepared	9 September 2020
Date Policy Approved by the Board / Management	15 September 2020
Date Policy became Operational	15 September 2020
Date of next review	15 September 2021

Introduction

Sotravic Limitee, a company registered under the law of Mauritius and having its registered office at Industrial Zone, La Tour Koenig, Mauritius, collects, uses, assesses, processes, stores, amends and transfers personal data in order to adopt and conduct the core business operations as required under their operating licensing requirements. Structured and unstructured data is processed by the Group on customers, clients, contractors, suppliers, business contacts, employees, and third-party stakeholders with which a business relationship is formed and created.

The Data Protection Policy ensures that the Group (Appendix 1):

- Complies with the data protection laws and regulations;
- Adopts and embeds a culture of data privacy best practices;
- Protects the rights of employees, customers, clients, contractors, partners and third-party stakeholders;
- Adopts a transparent approach in how it accesses, stores and processes individual information; and
- Protects itself from the risk of a data breach.

Scope

The Data Protection Policy is applicable to all the employees of the Group and consultants affiliated with third party stakeholders accountable and responsible for designing and operating the internal and external controls that protect the integrity, confidentiality and availability of the Group business data (structured and unstructured) and data locations (internal and external).

- This Data Protection Policy applies to all personal and sensitive data processed by the Group.
- The appointed Data Protection Officer acts as the responsible person and shall take responsibility for the ongoing compliance with this Data Protection Policy.
- This Data Protection Policy shall be reviewed at least annually.
- As a mandatory requirement under the GDPR and data protection legislations, the Group shall register with the appropriate Regulator as a Data Controller and notify the Regulator as to the details of the person nominated to monitor data protection compliance within the Group.

Data Protection Law

The Group is compliant to the GDPR, data protection laws and regulations where the Group resides. Where there is no such Data Protection Acts or data protection standards in a jurisdiction, the General Data Protection Regulation ("GDPR") prevails.

The GDPR and Data Protection Acts provides the legal framework in which the Group must handle, collect, store, amend and discard personal and sensitive data.

The GDPR and Data Protection Acts are applicable regardless of whether personal and sensitive data is stored electronically or in physical form. To ensure compliance with the GDPR and DPA, all personal and sensitive information must be lawfully collected, used fairly stored in a safe manner, transferred securely and not disclosed unlawfully. The Group provides for additional safeguards when processing sensitive information.

Definitions

Biometric Data	means any personal data relating to the physical, physiological or behavioural characteristics of an individual which allow his unique identification, including facial images or dactyloscopic data.
Consent	means any freely given specific, informed and unambiguous indication of the wishes of a data subject, either by a statement or a clear affirmative action, by which he signifies his agreement to personal data relating to him being processed.
Controller	means a person who or public body which, alone or jointly with others, determines the purposes and means of the processing of personal data and has decision making power with respect to the processing.
Data Subject	means an identified or identifiable individual, 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 individual.
DPA	means the Data Protection Act 2017 (Mauritius).
DPIA	means Data Protection Impact Assessment.
Data Protection Officer	means Data Protection Officer. The person responsible for data protection compliance.

4

Filing System	means a structured set of personal data which is accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.
GDPR	means the European Union General Data Protection Regulation.
Personal Data	means any information relating to a data subject.
Personal Data Breach	means 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.
Processor	means a person who, or public body which, processes personal data on behalf of a controller.
Processing	means an operation or set of operations performed on personal data or 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.
Profiling	means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.
Register of Data and Information Security Systems	means a register of all data and information security systems in which personal and sensitive data is processed by the Group.
Restriction of Processing	means the marking of stored personal data with the aim of limiting their processing in the future.
Special Categories of Data	in relation to a data subject, means personal data pertaining to: • his racial or ethnic origin; • his political opinion or adherence; • his religious or philosophical beliefs; • his membership of a trade union; • his physical or mental health or condition; • his sexual orientation, practices or preferences; • his genetic data or biometric data uniquely identifying him; • the commission or alleged commission of an offence by him; • any proceedings for an offence committed or alleged to have been committed by him, the

4

	disposal of such proceedings or the sentence of any Court in the proceedings; or • such other personal data as maybe determined to be sensitive personal data;
Third Party	means a person or public body other than a data subject, a controller, a processor or a person who, under the direct authority of a controller or processor, who or which is authorised to process personal data.
The Group	means Sotravic Limitee including its subsidiaries and affiliated entities.

Data Protection Principles

The GDPR and DPAs are underpinned with eight core principles on personal data:

- Be processed fairly and lawfully.
- Be obtained for only specific and lawful purposes.
- Be adequate, relevant and not excessive.
- Be accurate and kept up to date.
- Not be held for any longer than necessary.
- Processed in accordance with the rights of the data subjects.
- Be protected in appropriate ways.
- Not be transferred outside of the European Union unless that country or territory ensures an adequate level of protections.

The Group is wholly committed to processing and protecting personal and sensitive data and respecting the rights of data subjects in accordance with its responsibilities under the GDPRs and DPAs.

The DPA defines "Personal Data as:

- data which relate to an individual who can be identifies from those data; or
- data or other information, including an opinion forming part of a database, whether or not recorded in a material form, about an individual whose identity is apparent or can reasonably be ascertained from the data, information or opinion.

Article 5 of the GDPR requires that "Personal Data" shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organizational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

Lawful and Transparent Processing

The Group shall maintain a register of data and information security systems to ensure its processing of data is transparent and record the appropriate lawful basis of data processing. The register shall be reviewed at least annually. Individuals have the right to access their personal data and any such requests made to the Group shall be dealt with in a timely manner.

All personal data which is collected and processed by the Group under one of the following lawful purposes: legitimate interests, contract, legal obligation, vital interests, public task or contract.

The Group processes personal data in the interest of conducting and managing the business operations to enable our clients and stakeholders to have a service experience which is secure and does not have a negative impact on our clients and stakeholders' legitimate interests, namely with:

- Performance of a contract;
- Compliance with a regulatory or legal obligation;
- Compliance with a contractual obligation;
- Tendering, procurement structuring and management;
- Business development;
- Acting as an outsourced service provider;
- AML / CFT procedures;

Collection of Data

A Controller, shall not collect personal data unless –
(a) it is done for a lawful purpose connected with a function or activity of the Controller; and
(b) the collection of the data is necessary for that purpose.

- where a Controller collects personal data directly from a data subject, the Controller shall, at the time of collecting the personal data, ensure that the data subject concerned is informed of the identity and contact details of the Controller and, where applicable, its representative and any Data Protection Officer;
- the purpose for which the data are being collected;
- the intended recipients of the data;
- whether or not the supply of the data by that data subject is voluntary or mandatory;
- the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- the existence of the right to request from the Controller access to and rectification, restriction or erasure of personal data concerning the data subject or to object to the processing;
- the existence of automated decision making, including profiling, and information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject;
- the period for which the personal data shall be stored;
- the right to lodge a complaint with the Regulator;

4

- where applicable, that the controller intends to transfer personal data to another country and on the level of suitable protection afforded by that country; and
- any further information necessary to guarantee fair processing in respect of the data subject's personal data, having regard to the specific circumstances in which the data are collected.

Principles relating to processing of Data

The Group as a Controller or Processor shall ensure that personal and sensitive data is:

- processed lawfully, fairly and in a transparent manner in relation to any individual;
- collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data are erased or rectified without delay;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; and
- processed in accordance with the rights of the individual.

Data Controller – The Obligations

The Group is required to register as a Data Controller within their respective jurisdiction. Under the GDPR and DPA, it is the responsibility of the Group, as a Data Controller to be ultimately accountable for the implementation of all measurable technical and organizational data protection measures, namely:

- The implementation of data security measures;
- Appropriate record of processing;
- Performing a data protection impact assessment;
- Prior consultation to the Regulators in relation to the transfer of personal data to another jurisdiction in the absence of an appropriate safeguard(s); and
- Appointment of a designated responsible individual to act as a Data Protection Officer.

The GDPR and DPA provides that it is an offence for an organization to not have an appointed Data Protection Officer and not to register as a Data Controller.

Data Processor – The Obligations

A Data Processor is identified as any individual or public body that processes, uses and handles personal and sensitive data on behalf of the Group.

The GDPR and DPA provides that the Data Controller and Data Processor have a series of obligations which comprise that personal data is:

- Processed in accordance with the data subject rights;
- Processed lawfully, fairly and transparently with respect to the data subject;
- Collected for an explicit and legitimate purpose;
- Adequate, minimized and limited to the purpose(s) of processing;
- Kept and maintained accurately and rectified without undue delay; and
- Effectively stored and limited which permits the identification of the data subject.

CJ

Data Protection Officer

The Group has appointed a Data Protection Officer in order to monitor compliance with the GDPR and DPA. The appointment of the Data Protection Officer is to inform and advise the Group and the employees on their obligations to comply with the GDPR, DPA and data protection standards.

The Data Protection Officer has the professional experience and knowledge of data protection law and will be the key liaison officer with the employees and the Regulator. At any point in time, the Regulator may contact the Data Protection Officer for any required information about the Group's business operations as a Controller or Processor.

The Data Protection Officer is in place to monitor data compliance through:

- Exercising of the implementation of data privacy practices;
- Embedding a data privacy culture at The Group;
- Monitoring data breaches;
- Monitoring data subject access requests;
- Identifying and maintain segregation of data processed;
- Conducting data privacy awareness throughout the whole of the operations;
- Maintaining the data privacy policies and procedures, including the review of information security measures and safeguards.

The Data Protection Officer must work independently, report to the highest management level and have adequate resources to enable the Group to meet its obligations under the GDPR and DPA.

The following illustrates the minimum tasks that the Data Protection Officer must carry out in order to meet the business requirements at the Group:

- Monitor compliance with the GDPR and DPA, including managing internal data protection activities, advise on data protection impact assessments, train staff and conduct internal data privacy audits;
- Be the first point of contact for the Regulator and for individuals whose data are processed (employees, customers, contractors, suppliers, amongst others).

Data Privacy Notice

Where personal and sensitive data is collected by the Group from a data subject, by virtue of the Data Privacy Notice, the Group will inform the data subject on:

- The legal bases for processing;
- Sharing of personal data to third parties;
- Data Minimization;
- Data Accuracy;
- Data Security;
- Data Retention period;
- Data Subject rights; and
- Contact information pertaining to the Data Protection Officer at the Group.

The Group has published a Data Privacy Notice which is targeted to visitors on the website, customers, potential and existing clients, contractors, suppliers and third parties with whom the Group interacts with for the purpose of its business operations.

The Data Privacy Notice can be viewed on the website of the Group.

Consent

Consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data. Consent will be specific to each process that the Group is requesting consent for.

Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the Group's systems.

Data Minimization

The Group ensures that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Accuracy

The Group shall take reasonable steps to ensure personal data is accurate. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

Archiving

To ensure that personal and sensitive data is kept for no longer than necessary, the Group has put in place an archiving procedure for each area in which personal data is processed. The archiving procedure is reviewed bi-annually and shall consider what data must be retained, for how long, and why.

Security of Data

The Group ensures that personal and sensitive data is stored securely using an information security infrastructure that is regularly monitored and kept-up to date.

The Group will use appropriate measures to keep personal and sensitive data secure at all points of the processing to protect it from unauthorized or unlawful processing, or from accidental loss, destruction or damage.

Security measures to be adopted by the Group may include:

- Technical systems security;
- Information security measures to restrict or minimize access to personal and sensitive data;
- Access to personal data and sensitive shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorized sharing of information;
- Where personal and sensitive data is deleted this should be done safely such that the data is irrecoverable;
- Appropriate back-up and disaster recovery solutions shall be in place;
- Measures to ensure our systems and data remain available, or can be easily restored in the case of an incident;
- Physical security of information at the Group's office premises;
- Internal organizational measures, including data privacy policies, procedures, continuous awareness training and data privacy compliance audits;
- Regular testing of internal controls and evaluation of the effectiveness of security measures.

The Group adopts measures which include technical and organizational security measures. In assessing the most appropriate measures to protect personal data and safeguard against an ensuing data breach, the Group will consider all of the following factors:

- The quality of the security measure;
- The implementation costs;
- The nature, scope, context and purpose of processing;
- The risk to the rights and freedoms of a data subject; and
- The risk which could result from a data breach.

Data Retention Period

The Group will retain personal data for as long as is required and necessary in order to fulfil the lawful purposes with which the Group collects the personal data for, which will include satisfying any legal, regulatory compliance, tendering and procurement relationship, international reporting, information security, audit and accounting requirements and standards.

The Group determines the nature, sensitivity and context of the personal data, the potential risk of harm from unauthorized use or disclosure of personal data, the lawful purpose of processing in adherence to the appropriate legal requirements.

Data Subject Rights

The DPAs and Articles 15 – 22 (inclusive) provides that personal data will be processed in line with the rights of the data subject. The GDPR and DPA provides that a data subject has a series of rights, namely the right:

- Of access to data;
- To rectification of data;
- To restriction of processing;
- To object to processing;
- To data portability;
- To withdraw consent;
- To erasure or "to be forgotten"; and
- Not to be subject to automated decisions.

Data Subject Incident Response

Where the Group receives a request from a data subject that relates to their series of rights, the request will be forwarded to **[INSERT DESGINATED EMAIL ADDRESS]** whereby the designated Data Protection Officer will handle the request.

The Data Protection Officer will promptly act on all data subject requests by acknowledging receipt of the request then determining the validity of the request, reply to the data subject with the information requested by the data subject. It is to be clearly documented that any information provided to the data subject will be concise and transparent in nature, using clear and plan language. The appropriate timeframe to respond to a data subject request by the Group will be within a 30 days period. Should an extension be required to respond to the data subject request (namely, if there is an excessive amount of requests) or where information required to respond has to be gathered through various sources which can deem a delay in the response, The Group will duly inform the data subject that an extension of the timescale will be adopted and the circumstances notified to the data subject accordingly.

The DPA and Article 12 of the GDPR requires that a response to a Data Subject Access Request (DSAR) must be provided free of charge. Unless the data subject request is deemed to be manifestly unfounded, excessive or repetitive in nature, the Data Protection Officer at the Group level can either levy a reasonable fee taking into account the administrative burden associated with providing a response to the data subject or, as a last resort, refuse to act upon the request.

The Group has the right to refer any DSAR to the appropriate Regulator for further clarification.

Direct Marketing Practices

The Group complies with the DPA and GDPR which amend or replace the regulations on direct marketing and its practices. This includes, but is not limited, to, when the Group contacts a data subject by post, text message, social media messaging, telephone (recorded calls) and by facsimile.

Any direct marking material which the Group features as the sender will concisely describe how a data subject can object to receiving such communications identified in the previous paragraph in the future, If a data subject exercises their right to object to the direct marketing practices, then the Group will cease the direct marketing practice and the procedure will be handled by the Data Protection Officer at the Group and recorded accordingly in the register of data and information security systems. Additionally, the Marketing Department at the Group will be notified immediately so that a revision of the marketing practices can be identified and adopted.

Personal Data – Transfer

The Group has an international client base and business ventures. As a result, the Group has external third parties based outside of the European Economic Area and the Group may need to transfer personal data to other companies within the group solely in relation to the lawful purposes set out in this Data Protection Policy.
In the event that the Group transfers personal data, the Group ensures a similar degree of protection through the adoption and implementation of the following safeguards:

- The Group will only transfer personal data to countries that are deemed to have an adequate level of data protection;
- Where the Group has entered into a service agreement with a service provider, the Group may use specific contracts with a data security addendum which will afford the same level of data protection;
- The Group will refer the matter to the appropriate Regulator to ensure that additional safeguards can be met.

Data Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal and sensitive data, the Group shall promptly assess the risk to the data subject's rights and freedoms and, if appropriate, report a breach to the appropriate Regulators within 72 hours of knowing of the breach. All breaches should be escalated to the Data Protection Officer as the Group is accountable with the Regulator where the timeframe of 72 hours from being made aware of the data breach has lapsed. The Data Protection Officer will adopt the data breach communications strategy to minimize the damage and negative impact on the data subject.

4

Contact Information

Should you have any questions pertaining to this Data Protection Policy or have a request to be addressed contact the Data Protection Officer at the contact details provided below:

Appointed Data Protection Officer	Jurisdictional Coverage for GDPR and DPA
Name: Baker Tilly **Email:** Sotravic@bakertilly.mu **Telephone:** +230 460 8800 **By writing:** 1st Floor, CyberTower One, Ebene 72201, Mauritius	Mauritius

P.J.B.Ah

Approved By Chairman

P.J.B.Ah Sue

25/9/2020

Appendix 1: Sotravic Limitee, its subsidiaries and affiliated entities ('the Group")

Company	Address	Country
Sotravic Shared Services	Industrial Zone, La Tour Koenig	Mauritius
SBU 1 – Sotravic Infrastructure	Industrial Zone, La Tour Koenig	Mauritius
SBU 2 – Sotravic Waste & Energy	Industrial Zone, La Tour Koenig	Mauritius
SBU 3 – Sotravic International	Industrial Zone, La Tour Koenig	Mauritius
Subsidiary 1 – Sotravic Mechanical, Electrical and Plumbing (MEP) Ltd	Industrial Zone, La Tour Koenig	Mauritius
Subsidiary 2 – Sotravic Geotechnical Investigation Solutions	Industrial Zone, La Tour Koenig	Mauritius
Subsidiary 3 – Sotravic Equipment & Logistics – Armada Rental	Industrial Zone, La Tour Koenig	Mauritius