Data Protection Policy

harel mallac
for the better

HAREL MALLAC GROUP

DATA PROTECTION POLICY

1. INTRODUCTION

1.1. At Harel Mallac Group (the "**Group**"), we care about the way we use and process the personal data of: i. our employees; and ii. any other individuals – stakeholders, customers, suppliers, partners etc.

1.2. The Group and its Board of Directors are therefore committed to ensuring the safe and lawful processing of all personal data that it collects, in a fair and transparent manner, in accordance with applicable data protection laws in force, namely the Data Protection Act 2017 (Act No.20 of 2017) ("**DPA**") and the European General Data Protection Regulation ("**GDPR**").

1.3. This Policy sets out how personal data must be collected, processed and safeguarded in accordance with the law.

2. BACKGROUND

2.1. DATA PROTECTION ACT 2017

Under the DPA, we have a duty to ensure the lawful and fair processing of all personal data. There are **six (6) principles** in the DPA that constitute the core obligations of this Policy, to be adhered to, when processing personal data, as follows:

Personal data[1] must be:

1. processed lawfully and fairly;
2. collected and processed for a specific and lawful purpose;
3. adequate, relevant and not unnecessary;
4. accurate and up to date;
5. not be held for longer than is necessary;
6. processed in accordance with the rights of data subjects.

2.2. EU GENERAL DATA PROTECTION REGULATION

This regulation shall also apply under this Policy, when processing the personal data of any living human being within the EU, regardless of where the processing is being done.

2.3. What is personal data?

Personal data is any data from which, a living human being (known as a "data subject"- defined below) can be identified, such as (but not limited to): name, date of birth, ID Card No., postal and email address etc.

Personal data includes certain sensitive data known as "**special categories of personal data**" as follows:

"special categories of personal data", in relation to a data subject (defined below), means personal data pertaining to –

[1] *Exceptions to these or some of these principles may apply, such as (but not limited to) national security and public interest. Please consult the relevant data protection law.*

- his/her racial or ethnic origin;
- his/her political opinion or adherence;
- his/her religious or philosophical beliefs;
- his/her membership of a trade union;
- his/her physical or mental health or condition;
- his/her sexual orientation, practices or preferences;
- his/her genetic data or biometric data uniquely identifying him/her;
- the commission or alleged commission of an offence by him/her;
- any proceedings for an offence committed or alleged to have been committed by him/her, the disposal of such proceedings or the sentence of any Court in the proceedings; or
- such other personal data as the Data Protection Commissioner of the Ministry may determine to be sensitive personal data.

Personal data also includes children's personal data i.e. those aged less than 16 years.

2.4. What is processing of personal data?

"**Processing**" of personal data should be interpreted largely but includes 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, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

2.5. Who provides personal data?

This Policy shall apply to the personal data of all living human beings (known as "**data subjects**"), namely:

- All employees, trainees, volunteer workers of the Group; and
- Customers, suppliers, partners, shareholders, directors, officers and stakeholders of the Group etc.

3. PURPOSE OF THIS POLICY

3.1. The aim of this Policy is to: -

- Ensure compliance with applicable data protection laws and regulations in force;
- Follow good practice and foster a trustworthy environment for the processing of personal data of all stakeholders;
- Ensure transparency in the way that we process personal data;
- Protect the rights of individuals when processing their personal data;
- Prevent personal data from falling into the wrong hands;
- Protect the Group against any data privacy breaches and subsequent penalties and reputational damage.

4. OUR COMMITMENT

By endorsing this Policy, the Group and its directors commit to: -

- complying with applicable data protection laws and regulations in force;
- ensuring confidentiality of personal data;

- implementing good practice so as to ensure the trust of its stakeholders;
- processing personal data in an honest and transparent manner;
- protecting the rights of individuals when processing their personal data;
- protecting the Group against any data breaches and subsequent penalties and reputational damage.

5. APPLICABILITY OF THIS POLICY[2]

5.1. Who is under a duty to adhere to this Policy?

- All companies within the Group;
- Each Data Protection Officer designated by a company within the Group;
- All employees, trainees, volunteer workers of the Group;
- All directors and officers of the Group;
- All persons (known as "data processors") who have been appointed to process personal data on behalf of data controllers within the Group (defined below).

All companies within the Group are known as "**data controllers**" or "**controllers**" and may be referred to in this policy as "**the company**". Data controllers possess the decision-making power as to how and why personal data is collected. "**Data processors**" are third parties who may be appointed by data controllers to assist in the processing of personal data.

5.2. Specific duties:

Without limiting the responsibility of any other person or the following persons:

- The Board of Directors is ultimately liable for legal compliance by the company within the Group;
- Data Protection Officers have a duty to ensure compliance with this Policy and the applicable law of the company within the Group. This will include, attending to relevant queries regarding the protection of personal data, maintaining mandatory documents and audits for compliance to the privacy laws, ensuring the inclusion of relevant data protection clauses in contracts, the implementation of data processing agreements and any requests by data subjects (described below);
- IT managers have a duty to ensure the security and protection of personal data, through restricted access, adequate penetration testing, the safe storage of personal data e.g. on the cloud or an external server;
- Communication/Marketing Executives have a duty to ensure that there is no unlawful direct marketing (defined below) and that the rights to privacy of individuals are respected e.g. when displaying photos on the internet. They must also ensure the lawful processing of personal data through the Company's websites e.g. by prompting users to provide their tick the box consent to the use of cookies or for direct marketing, when filling in contact forms online.

6. OBLIGATIONS UNDER THIS POLICY

6.1. Responsibilities under the above-mentioned SIX (6) principles:

Personal data must be:

6.1.1. Principle 1: processed lawfully and fairly;

[2] *This Policy must be read in conjunction with the applicable laws and regulations in force especially regarding data protection and applied together with any other obligations of confidentiality and/or applicable IT/Security Policies.*

6.1.1.1. **Upon collecting personal data, the data subject must be informed of his or her rights, which will usually be set out in the Company's Privacy Notice/Policy.** This enables the data subject to take an informed decision prior to communicating his/her personal data. The data subject must therefore be informed of the following at the time of collecting his/her personal data[3]:

1. the identity and contact details of the controller and, where applicable, its representative and any data protection officer;
2. the purpose for which the data are being collected;
3. the intended recipients of the data;
4. whether or not the supply of the data by that data subject is voluntary or mandatory;
5. the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
6. 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;
7. 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;
8. the period for which the personal data shall be stored, or if a specific period cannot be provided, the criteria to determine that period should be provided;
9. the right to lodge a complaint with the Commissioner;
10. 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
11. 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.

6.1.1.2. **The processing of personal data must be processed in accordance with one of the following grounds for lawful processing:**

- **Consent** i.e. the data subject has given clear consent to process their personal information for a specific purpose
- **Contract** i.e. the processing is necessary for performance of a contract of the controller or its business units has with the data subject, or the data subject has requested the controller or its business units to take specific steps before entering into a contract
- **Legal obligation** i.e. the processing is necessary for the controller or its business units to comply with governing law
- **Vital interest** i.e. the processing is required to save the data subject's life
- Public task i.e. the processing is necessary for the controller and its business units in the public interest or official functions and the task or function has a clear basis in law
- **Legitimate interest** i.e. processing is necessary for the legitimate interest of the controller and its business units or the legitimate interest of a third party unless there is reason to protect the data subject's personal information which overrides legitimate interest.
- For the purpose of **historical, statistical or scientific research.**

6.1.1.3. **The processing of special categories of personal data requires additional conditions to be met to be considered lawful, namely:**

- Data subject has given explicit consent to the processing.

[3] *If the personal data was obtained from sources other than the data subject themselves, e.g. another company within the Group, the controller should provide the aforesaid privacy notice to the data subject at the latest upon the first communication with the data subject (if used for communication purposes, e.g. direct marketing) or within 1 month of obtaining the personal data for other form of processing.*

- Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law.
- Processing is necessary to protect the vital interest of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.
- Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body.
- Processing relates to personal data which are manifestly made public by the data subject.
- Processing is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity.
- Processing is necessary for reasons of substantial public interest.
- Processing is necessary for the purposes of preventive or occupational medicine.
- Processing is necessary for reasons of public interest in the area of public health.
- Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

6.1.1.4. Consent:

If consent has been identified as the lawful basis for the processing activity, the express and written consent (i.e. not implied) of the data subject must be obtained for the purpose of processing his or her personal data. In order to be considered lawful, consent should be:

- Freely given and affirmative
- Easily demonstrable
- Clearly distinguishable from other matters and not bundled with other clauses
- As easy to withdraw as it was to provide.

Personal data of children: The written consent of legal guardians of children must be obtained at all times before processing the personal data of their children e.g. if you are conducting a competition and/or prize giving for children. Any notice given in the context of processing personal data of children should be in a clear and plain language that the child can easily understand.

6.1.1.5. Legitimate Interest:

Prior to carrying out the processing of personal data under the basis of legitimate interest, a Legitimate Interest Assessment (LIA) should be performed to ensure that the rights of the data subjects are not being overridden. The LIA consists of three axes which must be considered, namely identifying the:

- Purpose of the processing activity;
- Necessity of the processing activity to accomplish the identified purpose;
- Balance between the legitimate interest of the company and the rights of the data subject.

The LIA must be documented and reviewed upon changes to the processing activity.

6.1.1.6. Direct marketing:

Prior to engaging in direct marketing with data subjects, the express and written consent (i.e. not implied) of the data subject must be obtained for his or her personal data to be processed for direct marketing. If personal data is collected online, this should be in the form of a tick the box consent together with acknowledgement of having read the privacy notice/policy.

"**Direct marketing**" means the communication of any advertising or marketing material which is directed to any particular individual.

6.1.1.7. Sharing of Client Databases:

Client databases must not be shared between companies in the Group or with any third party, unless a lawful basis for the transfer has been identified and validated by the Data Protection Officer of the Company. Binding rules between those different companies within the Group must be implemented and adhered to for the protection of such personal data. It is strictly forbidden to sell personal data to a third party without the written consent of the data subject.

6.1.1.8. Social media/advertising

The consent of the data subject must be obtained in writing before using his or her personal data such as (but not limited to) a photo taken of the data subject for advertising purposes or publication of latest news of the Group or announcement of a specific event, unless the consent is already present through a written agreement e.g. with a modelling company and the data subject, in a contract of employment or in the conditions of participation in an event. Such data will usually be accessible to the public at large e.g. through the social media. Hence, it is very important to respect the fundamental rights of privacy of the data subject. Data subjects must be given the chance to object to such processing of their personal data.

6.1.2. Principle 2: collected and processed for a specific and lawful purpose;

Personal data must only be used for a lawful purpose for which, it has been entrusted to us.

6.1.3. Principle 3: adequate, relevant and not unnecessary;

6.1.3.1. We must not ask for more personal data than is necessary. This is the principle of data minimization.

6.1.3.2. Special Categories of personal data must only be requested if essentially necessary.

6.1.4. Principle 4: accurate and up to date;

6.1.4.1. Personal data must be regularly checked and updated. If it is outdated, then the data must be destroyed, unless if required to be retained by law.

6.1.4.2. Companies must adopt user-friendly and accessible means for data subjects to inform them of any changes to their personal data.

6.1.5. Principle 5: not be held for longer than is necessary;

Companies within the Group must implement adequate retention policies regarding the different types of personal data that they hold. The retention periods must not in any event exceed any delays prescribed by law e.g. for accounting records or for court actions.

6.1.6. Principle 6: processed in accordance with the rights of data subjects.

6.1.6.1. The personal data must only be accessed by those requiring it for the purpose agreed to by the data subject.

6.1.6.2. Companies within the Group have a duty to ensure that its employees and all new recruits who are bound to comply with this Policy, receive the proper training in order to be able to handle and process personal data in accordance with this Policy.

6.1.6.3. Employees must consult their Data Protection Officer if they are unsure on how to handle personal data. Legal advice must be sought if need be.

6.2. Security of personal data

Each controller has a duty to ensure that personal data under its custody are appropriately safeguarded. This includes:

- documents containing personal data must (as far as is reasonably practicable) be password protected;
- printouts containing personal data that are no longer required must be shredded;
- printouts containing personal data must be locked in a filing cabinet or drawer and not accessible to unauthorized persons;
- measures must be implemented to ensure adequate back-up of personal data so that it is not lost and remains available in the event of a disaster;
- personal data must be protected from unlawful hacking. Sufficient and adequate penetration tests must be conducted. Adequate security software and firewall approved by the Company must be installed;
- mediums containing personal data must be protected by strong passwords;
- removable devices containing personal data must be locked in a filing cabinet or drawer when not in use;
- external servers or cloud systems storing personal data of the Company must be approved by the company beforehand with the relevant data processing agreement signed and in place in line with this Policy;
- computers/laptops/devices containing personal data must be locked when left unattended. Their screens must not be facing any unauthorized persons;
- each company within the Group must conduct regular self-assessments to verify the level of its compliance. Such assessments must be conducted in the event of any system changes e.g. ERP, new software, the collection of new types of personal data;
- Personal data must be adequately destroyed upon the lapse of any purpose for which, it is held and prompt instructions must be given to any data processor to also destroy such data in its possession and provide certification that same has been done.

In addition to the above, all persons processing personal data, to whom this Policy applies, are required to abide to the Group IT Policy, including but not limited to the following sections:

- Password policy
- Internet/Intranet Security Policy
- End-User Acceptable Usage policy
- Physical and Environment Security Policy
- Clean Desk and Clear Screen Policy
- IT Asset Retirement and Disposal Policy
- Backup Policy
- Bring Your Own Device Policy
- Removable Media Policy
- Laptop Security Policy
- Printer Policy
- Mobile Devices Policy
- Non-Disclosure Policy

6.3. Rights of data subjects

6.3.1. Data subjects are granted rights under the privacy laws which the controllers have a duty to respect where these are applicable[4].

6.3.2. Data subject have the right to:

- Know what personal data the controller holds on him/her
- Obtain a copy of his/her personal data
- Rectify any of his/her personal data
- Request for the erasure of his/her personal data
- Restrict the processing performed on his/her personal data
- Object to the processing of his/her personal data
- Request for his/her personal data to be ported to another data controller
- Not be subject to decision based solely on automated processing, e.g. profiling.

6.3.3. Companies in the Group have one month (30 days) to reply to requests of data subjects relating to their rights and must ensure that the relevant forms are available.

6.3.4. You must be satisfied as to the identity of any person claiming to be a data subject before granting him or her access to his/her personal data, rectifying and/or erasing his or her personal data.

6.3.5. Access to personal data must be granted to the data subject free of charge, unless such request is manifestly excessive e.g. requires excessive number of photocopies.

6.4. Transfer of personal data abroad

6.4.1. No personal data shall be transferred abroad:

- without the consent of the data subject (unless consent is not required- see "Consent" above and another lawful basis applies);
- it has explained to the data subject the risks involved in transferring his or her data abroad; and
- it can demonstrate the effectiveness of data protection safeguards in that country or the existence of legitimate compelling interests that outweigh the lack of such safeguards and would justify the transfer of such personal data abroad in such conditions.

6.5. Notification of a data breach

"Personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

6.5.1. Employees must notify their line managers and the Data Protection Officer of their employer immediately, in the event of any personal data breach. Data processors must notify the data controller immediately in writing of any personal data breach.

6.5.2. The data subject must be notified of any personal data breach with respect to his or her personal data where it would cause a high risk to his or her rights and freedom. There shall be no need to notify the data subject of such breach where:

[4] Data subjects' right may not be exercisable in all circumstances, e.g. data required to be retained by laws or regulations cannot be erased. Consult the Data Protection Officer of the company if you are unsure of the applicability of data subjects' right.

- such data is protected e.g. encrypted;
- such measures have been taken to eliminate the high risk;
- it would be disproportionate to notify e.g. where a public announcement of the breach has already been done.

6.5.3. The company must also assess whether the data breach causes a risk to the rights and freedom of the data subject, in which case the Data Protection Office (i.e. Data Protection Commission of the Ministry) is required to be notified within 72 hours of the company becoming aware of the breach. Factors to consider in the assessment include:

- Safeguards implemented around the data (e.g. encryption, anonymization etc.)
- Type of data involved in the breach
- Ease of identifying an individual with the information
- Severity of the breach
- Possible/anticipated receiver of the breach

6.6. Data Flow Management

Record of Processing Activity

6.6.1. Each company has the duty to identify all the processing activities performed on personal data falling under its responsibility. Following the identification of the processing activities, each company must document a **Record of Processing Activities (RoPA)** in enough detail to provide a complete overview of the flow of personal data within the company, including any transfers or disclosure. The RoPA must contain the following elements at a minimum:

- The name and contact details of the company and its Data Protection Officer
- The purposes of the processing activity
- A description of the categories of data subjects and of the categories of data related to personal information
- The lawful basis for processing and condition for processing special categories of personal data (as described above)
- Applicability i.e. whether the processing falls under the scope of GDPR or Mauritius DPA 2017 or both
- The categories of recipients to whom the personal data have been or will be disclosed
- Where applicable, transfers of personal data to a third country or an international organisation, and the documentation of safeguards implemented during the transfer
- The retention period of the data involved
- A general description of the technical and organisational security measures.

6.6.2. The RoPA must be maintained in a format which can be shared with the Data Protection Office of the Ministry upon request.

6.7. Data Protection Impact Assessment

6.7.1. Each company must ensure that a **Privacy Impact Assessment** is performed for all processing activities to determine the level of risk to the data subjects' rights and freedom. For all high risk activities or activities involving the tracking of individuals' online behaviour and which could result in a risk of physical harm in the event of a breach, a **Data Protection Impact Assessment (DPIA)** must be performed and documented by the company. The DPIA should contain the following elements at a minimum:

- Description of the nature, scope, context and purposes of processing

- Identification of existing measures that are in place for the mitigation of risks associated with the processing activities, including frequency of control, control owner, details of who performs the controls and who reviews the controls
- Assessment of whether the existing measures effectively mitigate the risks associated with the processing activities as well as residual risk acceptance level
- Assessment of whether additional measures need to be implemented to mitigate the risks associated with processing activities, including responsible party for implementation, deadline for implementation, additional budget required
- Consultation with the Commissioner or data subjects, if any was performed

The company must consult the Data Protection Office for guidance for instances whereby it cannot effectively mitigate high risks associated with processing activities.

7. ENFORCEABILITY OF THIS POLICY

7.1. Breach(es) of this Policy are likely to result in:

- heavy penalties and reputational damage for the Group and/or data controller i.e. applicable company within the Group and/or its employees, officers etc.
- an offence under the DPA or GDPR;
- disciplinary action and/or a legal action e.g. for damages against an employee who has committed the breach.
- civil and/or criminal legal action.

7.2. Any person in the company/Group, bearing the ultimate responsibility, for the commission of an offence under the DPA for which no specific penalty is provided or who otherwise contravenes that Act shall, on conviction, be liable to a fine not exceeding 200, 000 rupees and to imprisonment for a term not exceeding 5 years.

7.3. Any breach of the GDPR could result in heavy penalties i.e. fines amounting up to 4% of annual global turnover or €20 Million (whichever is greater).

8. REPORTING BREACHES:

8.1. Breaches of this Policy must be reported immediately in writing to the Managing Director and/or Data Protection Officer of the Company (data controller) in the Group concerned by the personal data.

8.2. The Group promotes openness and encourages all reporters to disclose their identity without fear of reprisal or victimisation. Anonymous reports will therefore, not be entertained. All persons required to comply with this Policy have a duty to ensure the proper implementation of this Policy for the good of all stakeholders (employees and non-employees) entrusting to us their personal data. Ensuring a trust-worthy environment can only increase stakeholder engagement and prosperity for our business.

Policy Information

Policy prepared by:	**Group Head of Legal Affairs**
Approved by the Board on:	**1st October 2018**
Policy came into effect on:	**1st October 2018**