Data Protection Policy

Data Classification: Public

The Agency for Infrastructure Malta

Version 1.2
March 2020

Data Protection Policy

Effective: 11th March 2020

Policy Owner: Data Protection Officer

Approved by: Board of Directors

Revision History			
Last Revised Date:	Last Revised By:	Last Approved By:	Revision Description:
20.03.2019	DPO	Board of Directors	Initial Version (v1.0.)
08.07.2019	DPO	DPO	Minor Change (v1.1.)
11.03.2020	DPO	DPO	Minor Change (v1.2.)

	Data Protection Officer Details
Data Protection Officer:	Dr Rachel Powell
Contact number:	+356 23341249
E-mail address:	dataprotection.im@infrastructuremalta.com

INFRASTRUCTURE MALTA

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Definitions

1.1.1 The following is a list of definitions for terms used throughout this policy.

- *Agency* – The Agency for Infrastructure Malta and the Agency refer and mean the same entity and are used interchangeably.
- *Consent* – means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he/she, either by a statement or by a clear affirmative action, signifies agreement to the processing of their personal data.
- *Criminal data* – means any personal data relating to criminal convictions and offences or related security measures. Criminal data relating to criminal offences and convictions is only processed by National Authorities.
- *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 being processed by the Data Controller and/or Data Processor.
- *Data Controller* – means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by EU or Member State laws, the Controller (or the criteria for nominating the Controller) may be designated by those laws. For the purposes of this Policy, the Agency for Infrastructure Malta is the designated Data Controller.
- *Data Processor* – means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the Data Controller. The Data Processor could also be the same Data Controller.
- *Data Protection Officer* – the Agency's data protection and data security leadership role required by the General Data Protection Regulation (GDPR). The Data Protection Officer is responsible for overseeing the Agency's data protection strategy and implementation to ensure compliance with GDPR requirements.
- *Data Subjects* – could be customers, suppliers, employees or other individual persons that interact with the Agency, and whose personal data is being processed by the Agency.
- *Personal Identifiable Information* – also referred to as PII and/or personal data means any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.
- *Processing* - means any operation or set of operations performed upon 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.

- *Pseudonymous Data* – treated as personal data as it enables the identification of individuals (albeit via a key). The 'key' that enables re-identification of individuals is kept separate and secure, the risks associated with pseudonymous data are likely to be lower, and so the levels of protection required for that data are likely to be lower.
- *Sensitive Personal data* – means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data.

2. POLICY STATEMENT, PURPOSE AND SCOPE

2.1.1 This Policy represents the policy for the Agency for Infrastructure Malta (the 'Agency') regarding the protection of personal identifiable information being processed whilst making aware the requirements of the General Data Protection Regulation (GDPR), as well as any underlying subsidiary legislation. The Policy also ensures that data subjects are aware of their rights.

2.1.2 This Policy enforces the responsibility on the Agency to:

- Comply with the Data Protection legislation, including good practice.
- Protect the data and information as well as the privacy rights of its data subjects (includes but is not limited to customers, employees, suppliers and other persons).
- Ensure that responsibilities to protect personal data are defined, communicated, implemented and effectively complied to.
- Manage the risks associated with the handling of personal data and the potential data breaches.
- To provide awareness training and support for the Agency's employees that handle and process Personal Identifiable Information.

2.1.3 This Policy applies to employees, interns, contractors and third parties of the Agency with the purpose:

- To outline how the Agency intends to comply with the GDPR and underlying regulations;
- To provide good practice guidance to its employees when handling and processing personal identifiable information;
- To protect the Agency from the consequences of any instances of non-compliance or breach of its responsibilities.

3. PRINCIPLES FOR PROCESSING PERSONAL DATA

3.1 Lawfulness, fairness and transparency

3.1.1 The GDPR requires that the Data Controller provide the data subject with information about his/her personal data processing in a concise, transparent and intelligible manner, which is easily accessible, distinct from other undertakings between the Data Controller and the data subject, using clear and plain language.

3.1.2 Transparency is achieved by keeping the data subject informed and this should be done before the data is collected and processed, and where and when any subsequent changes are made.

3.2 Purpose limitation

3.2.1 Processing personal data is only permissible if and to the extent that it is compliant with the original purpose for which the data was collected. Processing at a later point in time for “any other purpose” beyond the original intention requires further legal permission or consent. The only exception to this requirement is where the “other purpose” is “compatible” with the original purpose. Indications for this will be any link with the original purpose, the context in which the personal data has been collected, the nature of the personal data, the possible consequences of the intended further processing for data subjects or the existence of appropriate safeguards.

3.3 Data minimisation

3.3.1 The Data Controller shall ensure that only personal data which is necessary for each specific purpose is processed (in terms of the amount of personal data collected, the extent of the processing, the period of storage and accessibility). Under the GDPR, data must be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed". The Data Controller should not request data that goes beyond the purpose for which they are to collect and process.

3.4 Accuracy

3.4.1 Personal data must be accurate and kept up-to-date. Inaccurate or outdated data shall be deleted or amended, and the Data Controller is required to take "every reasonable step" to comply with this principle.

3.5 Storage limitation

3.5.1 Once the personal data is no longer required for the purpose for which it was collected, the Data Controller should ensure that it is deleted thereafter. In the event that the Agency has to retain the data for later use, it must ensure that it has sufficient grounds for doing so. In either case, when collecting the personal identifiable data, the data subjects are to be made aware of the full extent of data processing and data retention. This implies that there should be a regular review process in place with methodical cleansing of databases.

3.6 Integrity and confidentiality

3.6.1 Personal data must be protected against unauthorised access using appropriate organisational and technical measures. This goes to the heart of protecting the privacy of individuals. Data Controllers and Processors need to assess the risk, implement appropriate security controls for the data concerned and carry out regular checks that the data is up-to-date and working effectively. Anything falling short of this may result in a data breach, for which there are strict data breach provisions under the GDPR.

3.7 Accountability

3.7.1 The Data Controller must be able to demonstrate compliance with the general Data Protection principles. The range of processes that the Agency has in place to demonstrate compliance are:

- Developed a data privacy governance structure which includes a Data Protection Officer;
- Personal data set inventory;
- Appropriate privacy notices;
- Appropriate consent from data subjects, where applicable and/or required;
- Using appropriate organisation and technical measures to ensure that personal data is safe and secure;
- Using Privacy Impact Assessments; and
- Having in place a breach reporting mechanism.

3.8 Reliability of data processing

3.8.1 Collecting, processing and using personal data is permitted only under the following legal bases:

- Contractual agreement;
- Legal obligation;
- Legitimate interest;
- Consent;
- Explicit consent;
- Public interest task;
- Vital interest of the data subject;
- Employment / social security / social protection law;
- Collective agreement;
- Medical diagnosis by health professionals;
- Provision of health or social care or treatment;
- Not-for-profit organisations with a political, philosophical, religious or trade union aim;
- Public information;
- Judicial proceedings;
- Statistical / Historical / Research purposes.

3.8.2 One of these legal bases is also required if the purpose of collecting, processing and using the personal data is to be changed from the original purpose.

3.9 Customer Data

3.9.1 *Data processing:* The Data Controller may only appoint Data Processors which provide sufficient guarantees to implement appropriate technical and organisational measures to ensure processing meets the requirements of the GDPR. Data Processors are required to process personal data in accordance with the Data Controller's instructions. This imposes an indirect obligation for the Data Processor to comply with the same requirements that apply to the Data Controller, albeit at their instruction.

3.9.2 *Consent of data processing:* Data can be processed following consent by the data subject. The declaration of consent must be obtained in writing or electronically for the purposes of documentation. In some circumstances, consent can be given verbally and must be documented.

3.9.3 *Data processing pursuant to legal authorisation:* The processing of personal data is also permitted if national legislation requests, requires or allows this. The type and extent of data processing must be necessary for the legally authorised data processing activity and must comply with the relevant statutory provisions.

3.9.4 *Data processing pursuant to public interest:* Personal data can be processed if it is necessary:

i) to carry out a specific task in the public interest which is laid down by law; or

ii) in the exercise of official authority which is laid down by law.

No specific statutory power to process personal data is required, as long as, the underlying task, function or power has a clear basis in the law. Personal data may not be processed for the purposes of public interest if, the Data Controller could reasonably perform his tasks or exercise his powers in a less intrusive way.

3.9.5 *Data processing pursuant to legitimate interest:* Personal data can also be processed if it is necessary for a legitimate interest of the Agency for Infrastructure Malta. Legitimate interests are generally of a legal (e.g. collection of outstanding receivables) or commercial nature (e.g. avoiding breaches of contract). Personal data may not be processed for the purposes of a legitimate interest if, in individual cases, there is evidence that the interests of the data subject merit protection, and that this takes precedence. Before data is processed, it is necessary to determine whether there are interests that merit protection.

3.9.6 *Processing of highly sensitive data:* Highly sensitive personal data can be processed only if the law requires this or the data subject has given express consent. This data can also be processed if it is mandatory for asserting, exercising or defending legal claims regarding the data subject. If there are plans to process highly sensitive data, the Data Protection Officer must be informed in advance.

3.9.7 *Automated individual decisions:* Automated processing of personal data that is used to evaluate certain aspects, cannot be the sole basis for decisions that have negative legal consequences or could significantly impair the data subject. The data subject must be informed of the facts and results of automated individual decisions and the possibility to respond. To avoid erroneous decisions, a test and plausibility check must be made by an employee.

3.9.8 *User data and internet:* If personal data is collected, processed and used on websites or in apps, the data subjects must be informed of this in a privacy statement and, if applicable, information about cookies.

The privacy statement and any cookie information must be integrated so that it is easy to identify, directly accessible and consistently available for the data subjects.

If user profiles (tracking) are created to evaluate the use of websites and apps, the data subjects must always be informed accordingly in the privacy statement. Personal tracking may only be effected if it is permitted under national law or upon consent of the data subject. If tracking uses a pseudonym, the data subject should be given the chance to opt out in the privacy statement. If websites or apps can access personal data in an area restricted to registered users, the identification and authentication of the data subject must offer sufficient protection during access.

3.10 Employee data

3.10.1 *Data processing for the employment relationship:* In employment relationships, personal data can be processed if needed to initiate, carry out and terminate the employment agreement.

When initiating an employment relationship, the applicants' personal data can be processed. If the candidate is rejected, his/her data must be deleted in observance of the required retention period, unless the applicant has agreed to remain on file for a future selection process.

Consent is also needed to use the data for further application processes or before sharing the application with other *related* companies. In the existing employment relationship, data processing must always relate to the purpose of the employment agreement if none of the following circumstances for authorised data processing apply. If it should be necessary during the application procedure to collect information on an applicant from a third party, the requirements of the corresponding national laws have to be observed. In cases of doubt, consent must be obtained from the data subject.

There must be legal authorisation to process personal data that is related to the employment relationship but was not originally part of performance of the employment agreement. This can include legal requirements, collective regulations with employee representatives, consent of the employee, or the legitimate interest of the Agency.

3.10.2 *Data processing pursuant to legal authorisation*: The processing of personal employee data is also permitted if national legislation requests, requires or authorises this. The type and

extent of data processing must be necessary for the legally authorised data processing activity and must comply with the relevant statutory provisions. If there is some legal flexibility, the interests of the employee that merit protection must be taken into consideration.

3.10.3 *Collective agreements on data processing:* If a data processing activity exceeds the purposes of fulfilling a contract, it may be permissible if authorised through a collective agreement. Collective agreements are pay scale agreements or agreements between employers and employee representatives, within the scope allowed under the relevant employment law. The agreements must cover the specific purpose of the intended data processing activity and must be drawn up within the parameters of national data protection legislation.

3.10.4 *Consent to data processing*: Employee data can be processed upon consent of the person concerned. Declarations of consent must be submitted voluntarily. Involuntary consent is void. The declaration of consent must be obtained in writing or electronically for the purposes of documentation. In certain circumstances, consent may be given verbally, in which case it must be properly documented. In the event of informed, voluntary provision of data by the relevant party, consent can be assumed if national laws do not require express consent.

3.10.5 *Data processing pursuant to legitimate interest:* Personal data can also be processed if it is necessary to enforce a legitimate interest of the Agency for Infrastructure Malta. Legitimate interests are generally of a legal or financial nature.

Personal data may not be processed based on a legitimate interest if, in individual cases, there is evidence that the interests of the employee merit protection. Before data is processed, it must be determined whether there are interests that merit protection.

Control measures that require processing of employee data can be taken only if there is a legal obligation to do so or there is a legitimate reason. Even if there is a legitimate reason, the proportionality of the control measure must also be examined. The justified interests of the Agency in performing the control measure must be weighed against any interests meriting protection that the employee affected by the measure may have in its exclusion and cannot be performed unless appropriate.

The legitimate interest of the Agency and any interests of the employee meriting protection must be identified and documented before any measures are taken. Moreover, any additional requirements under national law must be taken into account.

3.10.6 *Processing of highly sensitive data:* Highly sensitive personal data can be processed only under certain conditions. Highly sensitive data is data about racial and ethnic origin, political beliefs, religious or philosophical beliefs, union membership, and the health and sexual life of the data subject. Under national law, further data categories can be considered highly sensitive or the content of the data categories can be filled out differently. Moreover, data that relates to a crime can often be processed only under special requirements under national law. The processing must be expressly permitted or prescribed under national law. Additionally, processing can be permitted if it is necessary for the Agency to fulfil its rights

and duties in the area of employment law. The employee can also expressly consent to processing. If there are plans to process highly sensitive data, the Data Protection Officer must be informed in advance.

3.10.7 *Automated decisions:* If personal data is processed automatically as part of the employment relationship, and specific personal details are evaluated (e.g. as part of personnel selection or the evaluation of skills profiles), this automatic processing cannot be the sole basis for decisions that would have negative consequences or significant problems for the affected employee. To avoid erroneous decisions, the automated process must ensure that a natural person evaluates the content of the situation, and that this evaluation is the basis for the decision. The data subject must also be informed of the facts and results of automated individual decisions and the possibility to respond.

3.10.8 *Telecommunications and internet.* Telephone equipment and e-mail addresses are provided by the Agency primarily for work-related assignments. They are a tool and an organisational resource. They can be used within the applicable legal regulations and internal Agency policies. In the event of authorised use for private purposes, the laws on secrecy of telecommunications and the relevant national telecommunication laws must be observed if applicable.

To defend against attacks on the IT infrastructure or individual users, protective measures can be implemented for the connections to the Agency for Infrastructure Malta network that block technically harmful content or that analyse the attack patterns. For security reasons, the use of telephone equipment, e-mail addresses and internet can be logged for a temporary period. Evaluations of this data from a specific person can be made only in a concrete, justified case of suspected violations of laws or policies of the Agency for Infrastructure Malta. The evaluations can be conducted only by investigating departments while ensuring that the principle of proportionality is met. The relevant national laws must be observed in the same manner as the Agency for Infrastructure Malta's regulations.

3.11 Third Party Suppliers

3.11.1 *Data processing:* Third Party Suppliers shall acknowledge that with respect to any Personal Data pertaining to the Agency for Infrastructure Malta, the Agency is the 'Data Controller' and the Supplier, the 'Data Processor'. The Data Controller strives to apply the appropriate technical and organizational security measures to protect any damage that might result from unauthorized or unlawful processing or accidental loss or destruction to personal data.

The Data Controller may only appoint Data Processors which provide sufficient guarantees to implement appropriate technical and organisational measures to ensure processing meets the requirements of the GDPR. Third Party Suppliers are required to process personal data in accordance with the Data Controller's instructions. This imposes an indirect obligation for the Third-Party Suppliers to comply with the same requirements that apply to the Data Controller, albeit at their instruction. The Data Controller endeavours to take reasonable steps to ensure compliance with those measures.

3.11.2 *Processing of highly sensitive data:* Highly sensitive personal data can be processed only under certain conditions. Highly sensitive data is data about racial and ethnic origin, political beliefs, religious or philosophical beliefs, union membership, and the health and sexual life of the data subject. Under national law, further data categories can be considered highly sensitive or the content of the data categories can be filled out differently. The Supplier shall take the appropriate physical, technical, organizational and administrative safeguards to protect the Data Controller's Sensitive Data against any Data Security Breach in accordance with the Privacy Laws.

3.11.3 *Data processing pursuant to contractual agreement:* The Data Controller shall ensure the processing is carried out under a written contract (Data Processing Agreement), under which the Data Processor is to act only on instructions from the Data Controller. Moreover, pursuant to applicable Privacy Laws, the Data Controller is required to obtain certain undertakings from its suppliers with regard to the collection, use, storage, disclosure, transfer and protection of the Controller's Personal Data.

3.11.4 *Supplier Personnel:* Only authorised Supplier personnel, who have a legitimate business need to meet the obligations under the Data Processing Agreement, shall be provided access to the Data Controller's Personal Data and such access should be limited to such parts of the Data Controller's Personal Data as is strictly necessary for performance of its duties under the Agreement. Supplier shall implement all measures reasonably necessary to ensure that its personnel are informed of the confidential nature of the Data Controller's Personal Data and comply with the obligations set out herein, including providing its personnel with the necessary training so that such persons can correctly, lawfully and safely process the Data Controller's Personal Data.

3.11.5 *Disclosure to Third Parties*: Supplier shall not be authorized to disclose or transfer the Data Controller's Personal Data to any third party without prior written approval of the Agency. Any such approval granted by the Agency may be subject to such conditions as it deems appropriate, including any requirement that the proposed third-party recipient of the Data Controller's Personal Data should enter into a data processing agreement directly with the Agency or with Supplier. Such data processing agreement may consist of EU Standard Contractual Clauses or terms that are substantially the same as the obligations contained herein. Supplier shall remain fully responsible for the acts and omissions of its agents, affiliates, vendors, subcontractors and/or any third party with whom it contracts or who processes the Data Controller's Personal Data on Supplier's behalf.

3.11.6 *Information Security:* Reference should be made to the Information Security Policy which applies to all employees and third party external entities performing work on behalf of the Agency for Infrastructure Malta.

4. NATIONAL TRANSMISSION OF PERSONAL DATA

Transmission of personal data to recipients outside or inside the Agency for Infrastructure Malta should only be allowed and carried out in line with the various policies and procedures pertaining to the specific relevant data set. The data recipient must be required to use the data only for the defined purposes. If data is transmitted by a third-party entity to the

Agency for Infrastructure Malta, it must be ensured that the data can be used for the intended purpose(s). Furthermore, all data sharing activities must be backed-up with an appropriate 'Data Sharing Agreement' between the parties.

5. INTERNATIONAL TRANSMISSION OF PERSONAL DATA

5.1.1 Transmission of personal data to recipients outside of the EU/EEA should only be allowed and carried out in line with the GDPR.

5.1.2 The IDPC recognises third countries which are, from time to time, recognised by the EU Commission to have an adequate level of protection. Data transfers to such third countries do not require a notification nor an authorisation by the IDPC. The list of countries enjoying an adequate level of data protection is published here: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en.

5.1.3 Data may still be transferred to the third country that does not ensure an adequate level of protection if:

- The data subject has given his or her unambiguous consent.
- It is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request.
- It is necessary for the performance or conclusion of a contract, concluded or to be concluded in the interests of the data subject between the controller and a third party.
- It is necessary or legally required on public interest grounds of for the establishment, exercise or defence of a legal claim.
- It is necessary in order to protect the vital interests of the data subject.
- It is made from a register that, according to laws or regulations, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, provided that the conditions laid down in law for consultation are fulfilled.

5.1.4 In certain circumstances where none of the derogations in Article 49 (1) apply, prior to transferring personal data to a third country, data controllers shall notify the Commissioner of such transfer of data resulting from a processing operation.

5.1.5 As per Article 47 (1) Binding Corporate Rules must also be submitted to the IDPC for approval.

5.1.6 A per Article 46 (3) the IDPC must authorise contractual clauses between the Controller or Processor and the Controller, Processor or the Recipient of the personal data in the Third Country or International Organisation.

5.1.7 In the absence of an appropriate safeguard data shall only be transferred to third countries if the IDPC is satisfied with the adequacy of the security after conducting an assessment in light of the purpose and duration of the proposed processing operation(s), the rules in force in the third country in question, as well as the professional rules and security measures which are complied with in that country. If not satisfied with the adequacy of security, the IDPC may prohibit the transmission of personal data. In such cases authorisation must be obtained.

5.1.8 If data is transmitted by a third party to the Agency for Infrastructure Malta, it must be ensured that the data can be used for the intended purpose. If personal data is transferred from the Agency for Infrastructure Malta to an entity with its registered office outside of the European Union/ European Economic Area, the entity importing the data is obliged to cooperate with any inquiries made by the relevant supervisory authority of the Agency for Infrastructure Malta, and to comply with any observations made by the supervisory authority with regard to the processing of the transmitted data.

6. RIGHTS OF THE DATA SUBJECT

6.1.1 All individuals who are the subject of personal data held and processed by the Agency for Infrastructure Malta have the following rights regarding data processing:

- *Right to be informed*: To attain information about the collection and use of their personal data;
- *Right to be forgotten*: To take action to erase their personal data;
- *Right to access*: To make subject access requests regarding the nature of information held and to whom it has been disclosed;
- *Right to rectification of processing*: To have inaccurate personal data rectified, or completed if it is incomplete;
- *Right to restrict processing*: To request the restriction or suppression of their personal data;
- *Right to data portability*: To obtain and reuse their personal data for their own purposes across different services, as well as to move, copy or transfer personal data easily from one entity to another in a safe and secure way, without hindrance to usability;
- *Right to object:* To object to processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling); direct marketing (including profiling); and processing for purposes of scientific/historical research and statistics;
- *Rights related to automated-decision making and profiling*: To be informed about the mechanics of automated decision-taking process that will significantly affect them, as well as to not have significant decisions that will affect them to be taken solely by automated process;
- *Right to free of charge service*: A proportional fee, taking into account the administrative costs of providing the information, may only be charged for access requests which are manifestly unfounded, excessive or repetitive;

- *Right to be notified of data breaches*: To attain information without undue delay in cases where a personal data breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms.

6.1.2 If a data subject contacts the Agency for Infrastructure Malta requesting information as to what and how their data is being processed, this is called a Subject Access Request (SAR).

6.1.3 Subject Access Requests from data subjects should be made via email, addressed to the Data Protection Officer sent to dataprotection.im@infrastructuremalta.com. The Data Controller can supply a standard request form, although individuals do not have to use this.

6.1.4 The Data Controller will always verify the identity of anyone making a Subject Access Request before handing over any information. Verification of identification procedures are defined in the Data Subject Verification Procedure.

7. CONFIDENTIALITY OF PROCESSING

7.1.1 Personal data is subject to data secrecy. Any unauthorised collection, processing, or use of such data by employees is prohibited. Any data processing undertaken by an employee without the necessary authorisation will not be allowed and will be considered as unauthorised. The "need to know" principle applies.

7.1.2 Employees may have access to personal information dependent on the appropriateness of the type and scope of the task in question. This requires a careful breakdown and separation, as well as implementation, of roles and responsibilities. Employees are forbidden to use personal data for private or commercial purposes, to disclose it to unauthorised persons, or to make it available in any other way. Supervisors must inform their employees at the start of the employment relationship about the obligation to protect data secrecy. This obligation shall remain in force even after their employment relationship has ended.

8. PROCESSING SECURITY

8.1.1 Personal data must be safeguarded from unauthorised access and unlawful processing or disclosure, as well as accidental loss, modification or destruction. This applies regardless of whether data is processed electronically or in paper form.

8.1.2 Prior to the introduction of new methods of data processing, particularly new IT systems, technical and organisational measures to protect personal data must be defined and implemented.

8.1.3 These measures must be based on the state of the art, the risks of processing, and the need to protect the data (determined by the process for information classification). In particular, the responsible department can consult with its Information Security Officer (ISO) and Data Protection Officer.

8.1.4 The technical and organisational measures for protecting personal data are part of Information Security Policy and must be adjusted continuously to the technical developments and organisational changes.

9. DATA PROTECTION IMPACT ASSESSMENT

9.1.1 Before carrying out any data processing which is likely to result in a high risk, the Agency will carry out a Data Protection Impact Assessment (DPIA) in line with Article 35 of the GDPR. The purpose is to help the Agency in identifying and assessing potential problems and mitigate or minimise privacy risks with data processing activities. Moreover, this shall form part of the principal obligation of the Data Controller to not simply act in compliance with the law but demonstrate such compliance (Article 5 of the GDPR)

9.1.2 DPIAs are not subject to the authorisation of the Commissioner. The controller shall only consult the supervisory authority prior to processing when, notwithstanding reasonable mitigating measures taken in terms of available technologies to address the high risks following the carrying out of a DPIA, residual high risks would still be present in the processing operation.

9.1.3 It is the responsibility of the Company to assess the risks to the rights and freedoms of data subjects and to identify the measures envisaged to reduce those risks to an acceptable level to demonstrate compliance with the GDPR. Such measures could include the use of appropriate technical and organisational security measures (effective full disk encryption, appropriate access control, etc).

9.1.4 When the Agency cannot sufficiently address and reduce the identified risks to an acceptable level (i.e. residual risks remains high), the supervisory authority (IDPC) must be consulted and obtain prior authorisation.

9.1.5 Regardless of whether or not consultation with the IDPC is required based on the level of residual risk, the obligation of retaining a record of the DPIA and updating the DPIA in due course remains.

9.1.6 In particular, the GDPR states that a DPIA must be conducted if the Agency plans to:

- use systematic and extensive profiling with significant effects;
- process special category or criminal offence data on a large scale;
- systematically monitor publicly accessible places on a large scale.

However, following the Opinion of the European Data Protection Board (EDPB), the Supervisory Authority also deems it appropriate to conduct a DPIA if the Data Controller plans to process personal data that involves:

- Systematic monitoring:

a) Observing, monitoring or controlling data subjects' behaviour, in particular, on the online environment;
b) Specific circumstances where the controller is legally required to process personal data about data subjects without their knowledge;
c) Operations concerning the use of geolocation data, including but not limited to, for the purpose of direct marketing;
d) Monitoring on a large scale of public spaces or private areas accessible by the public.

- Automated-decisions:
  e) e) fully or partially automated means of processing, including profiling, which produces legal effects concerning the data subjects or similarly significantly affects them.

- Use of innovative technologies:
  a) any processing of special categories of personal data and of data concerning vulnerable data subjects, through the use of innovative technologies or the implementation of new methods in existing technology.

- Special categories of data:
  a) processing on a large scale of special categories of data, including, personal data relating to criminal convictions and offences.

- Biometric data:
  a) any processing activity involving biometric data for the purpose of uniquely identifying data subjects:
     i. when the data subjects are in a public space or in a private area accessible to the public;
     ii. when the biometric data are processed in conjunction with personal data related to criminal convictions and offences;
     iii. when the biometrics are related to individuals who need high protection such as minors, employees, patients, mentally ill persons and asylum seekers.

- Genetic data:
  a) any processing of genetic data, other than that processed by an individual health care professional when providing a related service directly to the data subjects, for the purpose of matching or combining datasets in a way that would exceed the reasonable expectation of the data subject.

- Data concerning vulnerable persons:
  a) processing of personal data of vulnerable natural persons, in particular, concerning children, employees and individuals receiving any form of social assistance;

- Employee monitoring:
  a) processing of personal data for the purpose of the evaluation or scoring of aspects concerning the employee's performance at work, or when the processing increases the power imbalance between the data subjects and the data controller, particularly, when the employees may be unable to easily consent to, or oppose, the processing of their data or exercise their rights.

9.1.7 A DPIA shall begin early in the life of a project, before the processing even starts, and shall run alongside the planning and development process. It should include the following steps:

- Identify a need for a DPIA;
- Describe the processing;
- Consider consultation;
- Assess necessity and proportionality;
- Identify and assess the risks;
- Identify measures to mitigate the risks;
- Sign off and record outcomes;
- Integrate outcomes into plan;
- Keep under review.

9.1.8 The Agency has developed its own DPIA template for the purpose of conducting a data protection impact assessment on the basis of the guidelines issued by the IDPC.

9.1.9 The ultimate responsibility of conducting the DPIA falls on the Data Controller, however the Agency shall ensure the Data Protection Officer is overseeing the entire process and ensuring the DPIA is conducted in line with the Regulation.

9.1.10 A DPIA should be reviewed at least every 3 years, or sooner, depending on the nature of processing and the rate of change. The Agency shall keep in mind that the DPIA is an ongoing process and not a one-time exercise, this due to the change in risks and new vulnerabilities.

9.1.11 If the processing activity is, in part or in full, carried out by the Processor, the Processor is legally bound to assist the Controller by providing the necessary information.

10. DATA PROTECTION CONTROL

10.1.1 Compliance with the Data Protection Policy and the applicable data protection laws will be checked regularly with data protection audits and other controls.

10.1.2 The performance of these controls is the responsibility of the Data Protection Officer in conjunction with the other units within the Agency with audit rights or external auditors hired, as may be the case. The results of the data protection controls must be reported to the Data Protection Officer.

10.1.3 The Agency for Infrastructure Malta must be informed of the primary results as part of the related reporting duties. On request, the results of data protection controls will be made available to the Lead Supervisory Authority. The Supervisory Authority can perform its own controls of compliance with the regulations of this Policy, as permitted under national law.

11. DATA PROTECTION INCIDENTS

11.1.1 All employees must inform their supervisor or manager and the Data Protection Officer immediately about cases of violations against this Data Protection Policy or other regulations on the protection of personal data. The employee/manager responsible for the function or the unit is required to inform the Data Protection Officer immediately about data protection incidents, in cases of:

- Improper transmission of personal data to third parties;
- Improper access by third parties to personal data;
- Loss of personal data.
- Accidental or unlawful destruction of data; and
- Sending personal data to the wrong recipient.

Such reports must be made immediately so that any Incident Reporting obligations under the GDPR and/or National Law can be complied with.

12. RESPONSIBILITIES AND SANCTIONS

12.1.1 The “Process Owners” are responsible for data processing in their area of responsibility. These individuals are required to ensure that the legal requirements, and those contained in the Data Protection Policy, for data protection are met. Management staff are responsible for ensuring that organisational, HR, and technical measures are in place so that any data processing is carried out in accordance with data protection.

12.1.2 Compliance with these requirements is the responsibility of the relevant employees. If official agencies perform data protection controls, the Data Protection Officer must be informed immediately.

12.1.3 Management must ensure that their employees are sufficiently trained in data protection. Improper processing of personal data, or other violations of the data protection laws, can be criminally prosecuted in many countries and result in claims for compensation of damage. Violations for which individual employees are responsible can lead to sanctions under employment law.

12.2 Data Protection Officer

12.2.1 The Data Protection Officer, being internally independent of professional orders, works towards the compliance with national and international data protection regulations.

12.2.2 The Data Protection Officer is responsible for the Data Protection Policy and supervises its compliance. The Data Protection Officer is appointed by and reports directly to the Agency's Board of Directors.

12.2.3 Any data subject may approach the Data Protection Officer at any time to raise concerns, ask questions, request information or make complaints relating to data protection or data security issues.

12.2.4 If requested, concerns and complaints will be handled confidentially.

12.2.5 Decisions made by the Data Protection Officer to remedy data protection breaches must be upheld by the management of the Agency in question. Inquiries by supervisory authorities must always be reported to the Data Protection Officer.

12.3 Tasks of the Data Protection Officer

12.3.1 The Data Protection Officer shall have, as a minimum, the following tasks.

12.3.2 To inform and advise the Data Controller or the Data Processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;

12.3.3 To monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the Data Controller or Data Processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

12.3.4 To provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;

12.3.5 To cooperate with the Supervisory Authority;

12.3.6 To act as the contact point for the Supervisory Authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

12.3.7 The Data Protection Officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

13. SUPERVISORY AUTHORITY

13.1 Identification of the Lead Supervisory Authority

13.1.1 For the purposes of the GDPR, the Agency for Infrastructure Malta has identified the Office of the Information and Data Protection Commissioner of Malta as the Lead Supervisory Authority.

13.2 Notification to the Lead Supervisory Authority

13.2.1 In terms of Article 33 of the GDPR, in the case of a personal data breach, the Agency shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Lead Supervisory Authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the Lead Supervisory Authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

13.2.2 The notification (as detailed within the Incident Response Procedure) shall at least:

- describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned;
- communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
- describe the likely consequences of the personal data breach;
- describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

13.2.3 Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

13.2.4 All processors shall notify the Controller without undue delay after becoming aware of a personal data breach.

14. RELATED POLICIES

14.1 Data Retention & Archiving Policy

14.1.1 The Data Retention Policy includes standards, guidelines and procedures in respect to data retention periods for the various data sets identified and handled throughout the Agency.

14.2 Information Security Policy

14.2.1 The Information Security Policy includes standards, guidelines and procedures in respect to information security throughout the Agency.

14.3 Backup Policy

14.3.1 The Backup Policy includes standards, guidelines and procedures in respect to how backups are handled throughout the Agency.

14.4 Change Management Policy

14.4.1 The Change Management Policy includes standards, guidelines and procedures in respect to change management throughout the Agency.

14.5 Training Policy

14.5.1 The Training Policy includes the requirements for periodic training and compliance in relation to GDPR.

14.6 Compliance Programme

14.6.1 The Compliance Programme includes standards, guidelines and procedures in respect to ongoing compliance throughout the Agency.