IMPACT CREDIT GUARANTEE LIMITED
RC 1566879

A Subsidiary of Development Bank of Nigeria Plc

PRIVACY POLICY

September 2020

DOCUMENT REVIEW & APPROVAL

Document Name:	**PRIVACY POLICY**
Document Version:	Version 1.0
Document Description:	This document presents ICGL's Privacy policy. The policy is intended to establish how IMPACT handles the Personal Data of customers, suppliers, employees, workers and other third parties.
Created By:	Risk Management Department

1. Definition of Terms

- **Consent** of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
- **Data** means characters, symbols and binary on which operations are performed by a computer which may be stored or transmitted in the form of electronic signals is stored in any format or any device.
- **Database** means a collection of data organized in a manner that allows access, retrieval, deletion and procession of that data; it includes but not limited to structured, unstructured, cached and file system type databases.
- **Data Administrator** means a persons or organization that processes data.
- **Data Controller** means a person who either alone, jointly with other persons or in common with other persons or as a statutory body, determines the purposes for and the manner in which personal data is processed or is to be processed.
- **Data Portability** means the ability for data to be transferred easily from one IT system or computer to another through a safe and secure means in a standard format.
- **Nigeria Information Technology Development Agency** - NITDA
- **Data Protection Compliance Organization (DPCO**) means any entity duly licensed by NITDA for the purpose of training, auditing, consulting and rendering services and products for the purpose of compliance with this Regulation or any foreign Data Protection law or regulation having effect in Nigeria.
- **Data Subject** means an identifiable person; one who can be identified directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.
- **Party** means directors, shareholders, servants and privies of a contracting party.
- **Personal Data** means any information relating to an identified or identifiable natural person (data subject); an identifiable natural 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, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; It can be anything from a name, address, a photo, an email address, bank details, posts on social networking websites, medical information, and other unique identifier such as but not limited to MAC address, IP address, IMEI number, IMSI number, SIM and others.
- **Processing** means any operation or set of operations which is performed on personal data or on 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.
- **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.

- **Record** means public record and reports in credible news media.
- **Sensitive Personal Data** means data relating to religious or other beliefs, sexual tendencies, health, race, ethnicity, political views, trades union membership, criminal records or any other sensitive personal information.
- **Data Protection Impact Assessment** (often referred to as a DPIA)
- **The functions with** (**) fall under the Group Shared Services Agreement with the parent company (Development Bank of Nigeria Plc.).

2. Privacy Policy

IMPACT exists to alleviate financing constraints faced by Micro, Small and Medium Scale Enterprises (MSMEs) in Nigeria through providing partial credit guarantees and technical assistance to eligible Partner Financial Institutions on a sustainable basis. IMPACT`s services are provided at our Head Office, e-channels including the Internet. Also, Customers i.e. Partner Financial Institutions (PFIs) and potential customers can access the IMPACT`s services through other channels including its website www.impactguaranteeng.com

By accessing the IMPACT's services through the e-channels platform and or subscribing to any of its various products, IMPACT's customers provide certain personally identifiable information and information of consumers i.e. end borrowers

Also, IMPACT 's staff are required to provide certain personally identifiable information before, during and after recruitment. This document details the policies of IMPACT guiding the collection, use, storage, destruction and disclosure of this personally identifiable information.

This policy document would be made available on our website at www.impactguaranteeng.com . It shall be read thoroughly before accessing the IMPACT`s service. By accessing or subscribing to any of IMPACT's services, its consent to the processing of personal data in accordance with this policy.

a. Description of collectable personal information

IMPACT may ask for certain personally identifiable information that can be used to contact or identify an individual ("Personal Data") while using the Company's services or as a staff of IMPACT. Personally, identifiable information may include, but is not limited to:

ai. Name and Contact Data: IMPACT collects first, middle and last name, email address, bank verification number, postal address, phone number, signature, date of birth, an identification document such as a copy of driver's license, international passport, national identity card, and other similar contact data from its customers and staff. This includes data that does not name an individual but could potentially identify them. For example, a payroll or staff number. IMPACT shall ensure that staff are notified when any personal data they have in their possession will be used as its subject to the regulation.

aii. Credentials: When a PFI/MSME subscribes to any of the IMPACT's products, particularly our e-channels products, they may be required to provide a User ID, a password, details from a

token response device, password hints and similar security information used for authentication and account access.

They may also be required or opt to use biometric identification to access your account and authenticate transactions. While this information is required to ensure that they carry out transactions securely, appropriate security measures have been implemented to protect these data including encryption and storage in a secured environment, if required.

aiii. Usage Data: IMPACT may also collect information that the browser sends whenever customers access its online services and or when you access the services by or through a mobile device ("Usage Data").

This Usage Data may include information such as your computer's Internet Protocol address (e.g. IP address), browser type, browser version, the pages of the IMPACT `s Service that was visited, the time and date of the visit, the time spent on those pages, unique device identifiers and other diagnostic data.

When people access services by or through a mobile device, this Usage Data may include the following:

aiv. Geo-Location information: IMPACT may request access or permission to and track location-based information from your mobile device, either continuously or while you are using our mobile application, to provide location-based services. If you wish to change our access or permissions, you may do so in your device's settings.

av. Mobile Device Access: IMPACT may request access or permission to certain features from your mobile device, including your mobile device's camera, calendar, bluetooth, contacts, storage and other features. If you wish to change our access or permissions, you may do so in your device's setting.

aix. Mobile Device Data: IMPACT may automatically collect device information (such as your mobile device ID, model and Manufacturer), operating system, version information, IP address and diagnostic data.

b. Purpose of collection of personal data

The purpose of collecting personally identifiable information is to enable IMPACT to provide customers with the required services and ensure a lawful basis for handling any personal data of staff. The usage of data may be extended beyond the above whenever necessary for the purposes of meeting legal, regulatory, contractual obligations, and other legitimate business interests.

Specifically, the uses the Company could put data into include but not limited to:

- To provide and maintain services
- To notify about changes to service
- To provide customer care and support
- To provide analysis or valuable information so that we can improve our Service
- To monitor the usage of Service
- To detect, prevent and address technical issues
- To pay salary of staff,
- to carryout employment background checks
- to carryout investigation and detect crime

c. Technical methods used to collect and store personal information, cookies, JWT, web tokens etc.

To maintain the IMPACT `s security systems, protect staff, record transactions, and, in certain circumstances, to prevent and detect crime or unauthorized activities, IMPACT reserves the right to monitor all internet communications including web and email traffic into and out of its domains. The Company may use third-party Service Providers to monitor and analyze the use of Service provided e.g. Cookies.

ci. Cookies

To improve internet service, IMPACT may use a "cookie" and/or other similar files or programs which may place certain information on your computer's hard drive when you visit IMPACT web site. A cookie is a small amount of data that the IMPACT `s web server sends to your web browser when you visit certain parts of the Company`s site. IMPACT use analytics cookies to help understand how you use the Company`s site to discover what content is most useful to you. Cookies do not enable the IMPACT to gather personal information about you unless you give the information to the IMPACT `s server. Most Internet browser software allows the blocking of all cookies or enables you to receive a warning before a cookie is stored. For further information, please refer to your Internet browser software instructions or help screen. Alternatively, information on deleting or controlling cookies is available at www.allaboutcookies.org

d. Access (if any) of third party to personal data and purpose of access

IMPACT service may contain links to other sites that are not operated by the Company. If you click on a third-party link, you will be directed to that third party's site. IMPACT shall always advise through its website that Privacy Policy of every site is reviewed during visits.

IMPACT has no control over and assume no responsibility for the content, privacy policies or practices of any third-party sites or services.

IMPACT will take all steps reasonably necessary to ensure that data is treated securely and in accordance with this Privacy Policy. No transfer of Personal Data will take place to an organization or a country unless there are adequate controls in place including the security of the data and other personal information.

e. Available remedies in the event of violation of the privacy policy

In the event of a violation of the privacy policy, IMPACT would set up a Panel to investigate and ensure access, correction, deletion, or return of the individual's data in question) or employ other necessary measures to remedy the violation of the Principles only with respect to the individual.

f. The time frame for remedy

The remedy agreed with the Data Subject should be implemented within 1week to 3 months.

g. Any limitation clause

IMPACT would not incur any damages, costs, or fees.

3. Employee Privacy Policy

IMPACT is committed to protecting the privacy of its employees and other individuals employed by the Company or who apply for employment with IMPACT. The proper safeguarding of all personal employee information (i.e., personal information by which you can be identified) collected in the course of the Company's day-to-day activities is a cornerstone of this commitment. IMPACT adheres to the principles of the Nigeria Data Protection Regulation for the Protection of Personal Information to ensure that all information is properly collected, used

only for the purposes for which it was collected, and disposed of in a safe and timely manner when no longer needed.

OUR PRIVACY PRINCIPLES

1. Accountability

IMPACT is responsible for maintaining and protecting the personal employee information under its control. IMPACT has appointed a Data Protection Officer who is responsible for ensuring the Organization's compliance with its privacy obligations under this policy and the Nigeria Data Protection Regulation.

2. Identifying Purposes

IMPACT shall identify the purposes for which it is collecting personal employee information before this information is collected. Human resources staff collecting personal employee information on behalf of the Company should be able to explain to you the purposes for which the information is being collected.

3. Consent

All staff shall be informed and consent obtained for the collection, use and disclosure of their personal information, except where otherwise required or permitted by law. When it is appropriate, your written consent will be obtained.

4. Limiting Collection

IMPACT shall only collect the personal employee information that is reasonably required to meet the purposes of establishing, maintaining and concluding your employment. All such information shall be collected by fair and lawful means.

5. Limiting Use, Disclosure and Retention

Personal employee information shall only be used or disclosed for the purpose(s) for which it was reasonably collected unless you otherwise consent or when it is required or permitted by law. Personal employee information shall only be retained for the period of time required to fulfill the purposes for which it was collected and for a period of seven (7) years after employment ceases.

6. Accuracy

Personal employee information shall be maintained in as accurate, complete and up-to-date form as is reasonably necessary to fulfill the purposes for which it was collected.

7. Safeguards

Personal employee information shall be protected by adequate security safeguards. Safeguards include physical measures such as locked filing cabinets, organizational measures such as security clearances, and technological measures such as the use of passwords and encryption. IMPACT shall work to ensure that its human resources employees and other employees are aware of the importance of maintaining the confidentiality of personal employee information.

8. Openness

IMPACT shall make available to you, all relevant information about its policies and practices that apply to the management of your personal employee information.

9. Individual Access

Upon request, you shall be informed of the existence, use and disclosure of your personal employee information and be given access to it, except when prohibited by law. You may verify the accuracy and completeness of your employee personal information, and may request that it be amended, if appropriate. Requests for access to your personal information may be made to the Head of Human Resources (**).

10. Compliance

Any questions or concerns with regards to the Company's compliance (with) these Privacy Principles may be directed to the IMPACT's Data Protection Officer at: +234-9 904 0000 ext. 3005.

4. Data Security and Storage

IMPACT recognizes the importance of protecting data from unauthorized access and data corruption and the Company shall:

- Develop security measures including but not limited to protecting systems from hackers
- Set up firewalls and protect email systems
- Store data securely with access to specific authorized individuals
- Employ data encryption technologies
- Develop organizational policy for handling personal data and other sensitive or confidential data
- Continuously build capacity for all staff

a. Network Access Control

IMPACT has deployed a number of solutions to prevent unauthorized access into the Company's networks. This will help in curbing and knocking off rogue systems from gaining access. There is an authentication mechanism deployed in the Company's domain to allow only authenticated users gain access to the network. It also keep tabs of workstation activities and reporting mac addresses connected to a particular port at any given time.

b. Intrusion Prevention System

IMPACT has set up layers of security devices, controls and protocol in order to prevent intrusions. A Security Information and Event Management System is deployed to monitor network traffic in the Company's domain. There is also a machine learning mechanism which reports changes in behavior of traffic, brute force attacks, access and changes made on applications and system, rogue scan tools and also detects malwares running on any workstation/server.

c. Endpoint Security System

Endpoint security and protection is an approach IMPACT takes to protect its server systems and client devices. It includes securing endpoints, or end-user devices like desktops, laptops, and mobile devices which serve as points of access to the Company's enterprise network and create points of entry that can be exploited by malicious actor. IMPACT ensures that all these actors are covered within its domain in order to prevent unfavorable and unwanted behaviors.

d. Data Backup

IMPACT backs up data from its core applications daily and ensure all personal information are stored in the cloud. These are tested routinely.

e. Hardware Encryption

There are a series of full volume encryption approached designed in order to protect data by providing an encryption methodology which encrypt the entire system volume using Advanced Encryption Standard (AES) encryption algorithm. IMPACT leverages on these types of encryption frameworks to protect all its assets.

f. Physical Security

IMPACT physical security aims at providing a layered approach to physical security, which will provide a suitably secure environment. This is to prevent unauthorized physical access, damage, and interference to the organization's premises and information.

In line with the Group's information security policy, IMPACT's office & facilities shall be kept secured at all times in order to prevent unauthorized access, damage and interference to IMPACT's premises and information. cameras, locks and/or other automated controls shall be used to limit access to the data center and other secure areas.

5. Third Party Data Processing

IMPACT's website may contain links to third-party websites, products and services. Information collected by such third parties which may include such things as location data or contact details shall be governed by the privacy practices and policies of the third parties, and IMPACT will not be liable for any breach of confidentiality or privacy of your data on such sites. You are advised to learn about the privacy practices of those third parties.

Generally, staff are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

Staff may only share the Personal Data we hold with another employee if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

Staff may only share the Personal Data we hold with third parties, such as our service providers, if:

- they have a need to know the information for the purposes of providing the contracted services;
- the Data Subject's Consent has been obtained;
- the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
- the transfer complies with any applicable cross-border transfer restrictions; and
- a fully executed written contract that contains NDPR-approved third party clauses has been obtained.

The contracts with third parties handling personal information include clauses on the right to audit security technologies are implemented to enforce encryption.

IMPACT shall, at its discretion, monitor usage of its information assets as per applicable laws and terms and conditions of employment agreed upon by IMPACT and the employee/contractor/third party personnel. This may include, but not limited to; logging and reviewing of user activity such as telephone numbers dialed, web sites visited from IMPACT owned assets and electronic communications exchanged through IMPACT's information processing facilities and networks. Legal advice shall be sought in writing prior to monitoring the personal information of the user/customer and record of the same shall be maintained.

6. Internal Sanctions

Any person subject to this policy failing to comply with the general provisions set out above or specific issues which are dealt with in this policy or any amendment thereto shall render him/her liable to appropriate disciplinary or legal action.

Breach of this Policy will be considered a serious disciplinary matter and will be dealt with in accordance with the Group's Disciplinary Procedure. The specific discipline imposed will be determined on a case-by-case basis, taking into consideration the nature and severity of the violation, prior violations of the policy, regulations, laws and all other relevant information.

In a case where an individual that violates this policy is not an employee of IMPACT the matter shall be submitted to the Internal Audit (**) team. The Internal Audit (**) team may refer the information to law enforcement agencies and/or law agencies for consideration as to whether criminal charges should be filed against the alleged violator(s).

All information security incidents will be sanctioned except where it was clearly established that it was unintended or accidental which may attract lesser sanctions include e.g. mandatory class training or as determined by Human Resources Unit (**).

In less serious cases you may have access to the internet removed or other disciplinary action taken against you, short of dismissal. All cases shall be determined following the Disciplinary Committee (DC) process, except issues that attract departmental warning letter.

Management is at liberty to dispense sanctions as it deems fit without restraint to the Group's disciplinary procedure.

7. Transfer to a Foreign Country

IMPACT restricts data transfers to countries outside Nigeria and international organizations to ensure that the level of data protection afforded to individuals by the NDPR is not undermined. IMPACT shall only transfer Personal Data outside Nigeria or to an international organization if one of the following conditions applies:

- the Data Protection Authority of Attorney General of the Federation has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subject's rights and freedoms;
- the transfer is necessary for one of the other reasons set out in the NDPR including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest.

8. Awareness and Training

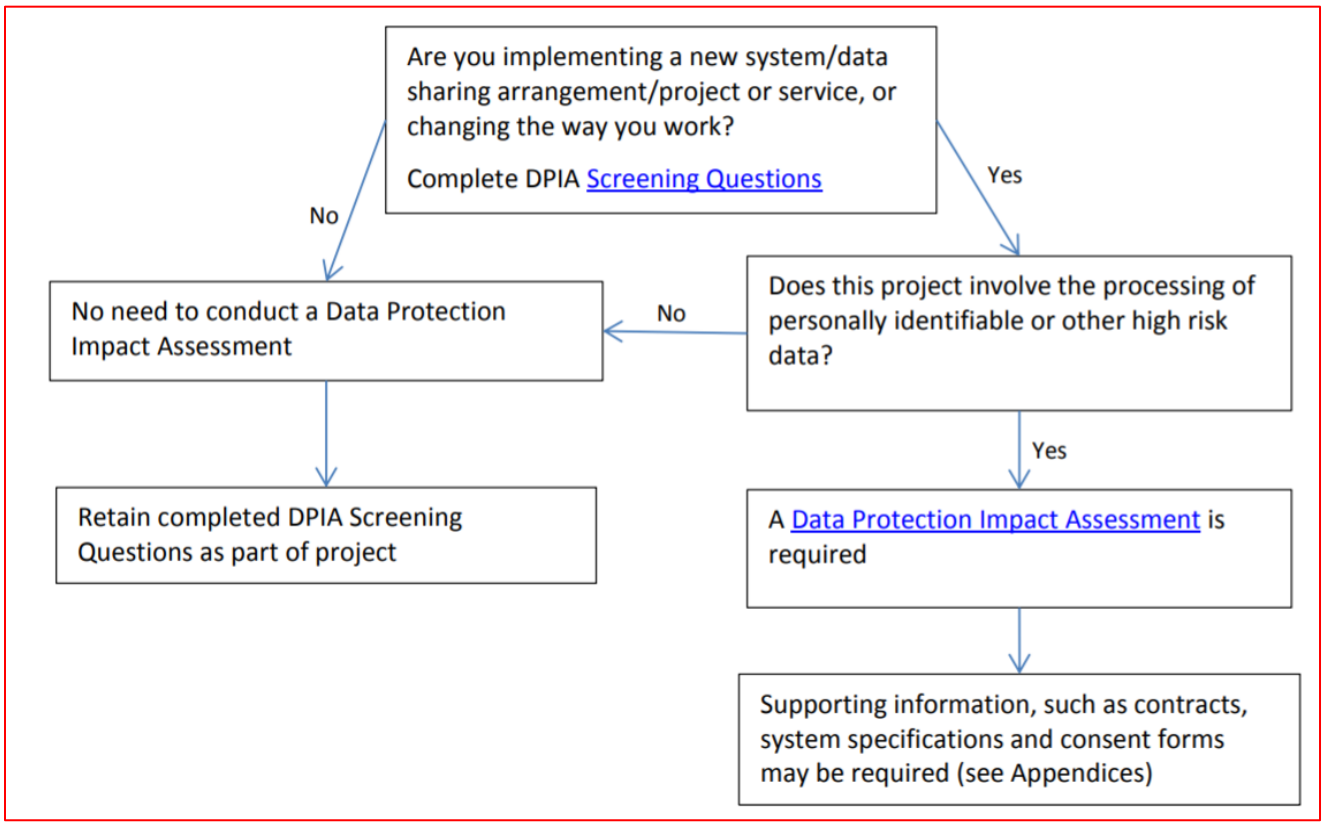
All staff shall be made aware of the Data Protection Regulation and Privacy Policy and their responsibilities for the protection of personal data. All staff and the DPO shall acknowledge their awareness, understanding and compliance with this Policy.

9. Data Protection Impact Assessment

A Data Protection Impact Assessment (often referred to as a DPIA) is a process or task designed to identify what data protection issues may arise from certain 'high risk' projects we are undertaking.

A 'high risk' project is one where the processing of personal data is likely to result in infringing of rights and freedom.

The DPIA will help the Company manage any risk by allowing us to identify the risk, and to implement solutions to those risks project at an early stage.



DPIAs should be completed where a system/data sharing/project includes the use of personal data, where there is otherwise a risk to the privacy of the individual, utilization of new or intrusive technology, or where private or sensitive data which was originally collected for a limited purpose will be reused in a new and 'unexpected' way.

10. Communication of Personal Data Breach

Where the Personal Data breach is likely to result in a high risk to the rights and freedoms of Data Subjects, the Data Controller shall communicate the Personal Data breach to the Data Subject without undue delay in any case not later than 72 hours/3 days.

The communication to the Data Subject shall describe in clear and plain language the nature of the Personal Data breach and contain at least the information and measures referred to in Section 13.

The communication to the Data Subject shall not be required if any of the following conditions are met:

- the Data Controller has implemented appropriate technical and organizational protection measures, and those measures were applied to the Personal Data affected by the Personal Data breach, in particular those that render the Personal Data unintelligible to any person who is not authorized to access it, such as encryption;
- the Data Controller has taken subsequent measures to ensure that the high risk to the rights and freedoms of Data Subjects are no longer likely to materialize;
- it would involve disproportionate effort. In such a case, the Data Controller shall issue a public communication or similar measure whereby the Data Subjects are informed in an equally effective manner
- Where the Data Controller has not communicated the Personal Data breach to the Data Subject, the Supervisory Authority, having considered the likelihood of the Personal Data breach resulting in a high risk, may order the Data Controller to make such communication or declare that any of the conditions referred to above are met.

11. Notification of a Personal Data breach

In the case of a Personal Data breach, the Data Controller shall without undue delay and, where feasible, not later than 72 Hours/3 days after having become aware of it, notify the Personal Data breach to the CBN and NITDA, unless the Personal Data breach is unlikely to result in a risk to the rights and freedoms of Data Subject. Any notification to the CBN and NITDA outside the specified time frame, shall be accompanied by reasons for the delay.

The notification referred to above 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 Data Controller or Processor as the case may be to address the Personal Data breach, including, where appropriate, measures to mitigate its possible adverse effects.
- 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.
- The Data Controller shall document any Personal Data breaches, comprising the facts relating to the Personal Data breach, its effects and the remedial action taken. That documentation shall enable the CBN and NITDA to verify compliance with this Regulation.

12. Internal Audit (**)

The Internal Audit Department (**) as part of its annual audit shall conduct a detailed audit of the IMPACT's privacy and data protection practices with at least each audit stating:

- personally identifiable information IMPACT's collects on employees and members of the public;
- any purpose for which the personally identifiable information is collected;
- any notice given to individuals regarding the collection and use of personal information relating to that individual;
- any access given to individuals to review, amend, correct, supplement, or delete personal information relating to that individual;
- whether or not consent is obtained from an individual before personally identifiable information is collected, used, transferred, or disclosed and any method used to obtain consent;
- the policies and practices of IMPACT's for the proper use of personally identifiable information;
- IMPACT's policies and procedures for privacy and data protection;
- the policies and procedures of IMPACT's for monitoring and reporting violations of privacy and data protection policies; and
- the policies and procedures of IMPACT's for assessing the impact of technologies on the stated privacy and security policies.

Where a Data Controller processes the Personal Data of more than 1000 in a period of six months, a soft copy of the summary of the audit containing information stated above shall be submitted to NITDA.

On annual basis, a Data Controller who processed the Personal Data of more than 2000 Data Subjects in a period of 12 months shall, not later than the 15th of March of the following year, submit a summary of its data protection audit to the Agency. The data protection audit shall contain information as specified above.

13. Changes to Privacy Policy

IMPACT's reserves the right to amend its prevailing Data Protection and Privacy Policy at any time and will place any such amendments as it occurs on its Web Site. This Data Protection and

Privacy Statement is not intended to, nor does it create any contractual rights whatsoever or any other legal rights, nor does it create any obligations on IMPACT in respect of any other party or on behalf of any party.