CONTENTS

Introduction

These guidelines are mainly inspired from opinion 02/2013 on apps on smart devices of Article 29 Data Protection Working Party.

Apps include activities such as web browsing, communication (e-mail, telephony and internet messaging), entertainment (games, movies/video and music), social networking, banking and location based services. Apps can collect large quantities of data from the device (e.g. data stored on the device by the user and data from different sensors, including location) and process them in order to provide services to the end user. However, the same data sources can be further processed, in ways unknown or undesired by the end user.

App developers may pose consequential threats to the private life and reputation of users of smart devices if they do not comply with data protection laws. The key data protection risks to end users are the lack of transparency and awareness of the types of processing an app may undertake combined with a lack of free and informed consent from end users before that processing takes place.

Many apps do not have a privacy policy or do not inform their potential users in a user-friendly way about the types of personal data the app may process and for what purposes. Once the app is downloaded, consent is often reduced to a tick box indicating that the end user accepts the terms and conditions, without even offering a 'No thank you' option.

Poor security measures may lead to unauthorised processing of personal data, for example, if an app developer commits a personal data breach. Disregard for the principle of purpose limitation, which requires that personal data may only be collected and processed for specific and legitimate purposes, is another data protection risk. Personal data collected by apps may be widely distributed to a number of third parties for undefined or elastic purposes such as 'market research'. An apparent trend towards data maximisation and the elasticity of purposes for which personal data are being collected further contribute to the data protection risks found within the current app environment.

A high risk to data protection also stems from the segregation of roles between the various players in the app development landscape. They include: app developers who create apps and/or make them available to end users; app owners; app stores; Operating System and device manufacturers (OS and device manufacturers); and other third parties that may be involved in the collection and processing of personal data from smart devices, such as analytics and advertising providers. Although App developers have the greatest control over the precise manner in which the processing is undertaken or information presented within the app, often, in order for them to achieve the highest standards of privacy and data protection, they have to collaborate with other parties in the app ecosystem. This is particularly important with regard to security, where the chain of multiple actors is only as strong as its weakest link.

Data Protection Principles

In order to identify the potential data controller/s, sections 3(3), (4) and (5) of the Data Protection Act (DPA) are relevant:-

(3) Subject to Part VII, this Act shall apply to a data controller -

a) who is established in Mauritius and processes data in the context of that establishment;and
b) who is not established in Mauritius but uses equipment in Mauritius for processing data, other than for the purpose of transit through Mauritius.

(4) A data controller, falling within subsection (3)(b) shall nominate for the purposes of this Act, a representative established in Mauritius.

(5) For the purposes of subsection (3)(a) any person who -

a) is ordinarily resident in Mauritius;
b) carries out data processing activities through an office, branch or agency in Mauritius,

shall be treated as being established in Mauritius.

The concept of "establishment" is crucial in determining whether the DPA is applicable. An organisation XYZ is involved in the development of apps for Country A but XYZ is geographically located outside Country A. XYZ should consider that all the requirements of apps must comply with data protection laws of Country A.

Personal data

Many types of data available on a smart mobile device are personal data. Therefore, the DPA applies. They are personal data whenever they relate to a living individual, who is directly (such as by name) or indirectly identifiable to the controller or to a third party. They may relate to the owner of the device or to any other individual, such as the contact details of friends in an address book. Data can be collected and processed on the device or, once transferred, elsewhere, on app developers' or third parties' infrastructure, via connection to an external API, in real-time without the knowledge of the end user.

Examples of such personal data that can have a significant impact on the private lives of the users and other individuals are:

- Location
- Contacts
- Unique device and customer identifiers (such as International Mobile Equipment Identity (IMEI), International Mobile Subscriber Identity (IMSI), Unique Device Identifier (UDID) and mobile phone number)
- Identity of the data subject
- Identity of the phone (i.e. name of the phone)
- Credit card and payment data
- Phone call logs, SMS or instant messaging
- Browsing history
- Email
- Information society service authentication credentials (especially services with social features)
- Pictures and videos
- Biometrics(ex:-facial recognition and fingerprint templates)

Consent

Consent to process personal data must have 3 characteristics as per section 2 of the DPA:-

In the context of smart devices, a 'freely given' consent means that a user must have the choice to accept or refuse the processing of his personal data. Therefore if an app needs to process personal data, a user must be free to accept or refuse. The user should not be confronted with a screen containing only a 'Yes I accept' option in order to finish the installation. An option to 'Cancel' or otherwise stop the installation must be available.

'Informed' means that the data subject must have the necessary information at his end in order to form an accurate judgment. In order to avoid any ambiguity, such information must be made available before any personal data is processed. This includes data processing that could take place during installation, for example, for debugging or tracking purposes.

'Specific' means that the expression of consent must relate to the processing of a particular data item or a limited category of data processing. It is for this reason that simply clicking an "install" button cannot be regarded as valid consent for the processing of personal data due to the fact that consent cannot be a blanket authorisation. In some cases users are able to give a granular consent, where consent is sought for each type of data the app intends to access. Such an approach achieves two important legal requirements, firstly of adequately informing the user about important elements of the service and secondly asking for specific consent for each. The alternative approach for an app developer asking its users to accept a lengthy set of terms and conditions and/or privacy policy does not constitute specific consent. Specific means that the consent must be limited to the specific purpose of advising the user about a particular product. The location data from the device may therefore only be accessed when the user is using the app for that purpose. The user's consent to process geolocation data does not allow the app to continuously collect location data from the device. This further processing would require additional information and separate consent.

Similarly, for a communication app to access the contact list, the user must be able to select contacts that the user wishes to communicate with, instead of having to grant access to the entire address book (including contact details of non-users of that service that cannot have consented to the processing of data relating to them).Specific also relates to the practice of tracking user behaviour by advertisers and any other third party. The default settings provided by OSs and apps must be such as to avoid any tracking, to allow users to give specific consent to this type of data processing. These default settings may not be circumvented by third parties, as is currently often the case with "Do Not Track" mechanisms implemented in browsers.

It is important to note however that even if the consent meets the three elements described above, it is not a license for unfair and unlawful processing to take place. If the purpose of the data processing is excessive and/or disproportionate, even if the user has consented, the app developer will not have a valid legal ground and would be in violation of the DPA.

Contractual legal ground

An exception under section 24 or 25 of the DPA:-

For example, a user consents to the installation of a mobile banking app. In order to fulfill a request to make a payment the bank does not have to ask for the separate consent of the user to disclose his name and bank account number to the recipient of the payment. This disclosure is strictly necessary in order to perform the contract with this specific user, and therefore the bank has a legal ground under section 24(2) (a) or section 25 (2) (a) (iv) of the Data Protection Act concerning sensitive personal data. The same reasoning applies to communication apps; when they provide essential information such as an account name, e-mail address or phone number to another individual that the user wishes to communicate with, the disclosure is obviously necessary to perform the contract.

Purpose limitation and data minimisation

Purpose limitation enables users to make a deliberate choice to trust a party with their personal data as they will learn how their data are being used, and will be able to rely on the limitative purpose description to understand for what purposes their data will be used. The purposes of the data processing therefore need to be well-defined and comprehensible for an average user without expert legal or technical knowledge. Personal data may only be processed for fair and lawful purposes according to the DPA and these purposes must be defined before the data processing takes place.

For example, if an app originally had as purpose to allow users to e-mail each other, but the developer decides to change its business model and merges the e-mail addresses of its users with the telephone numbers of users of another app. The respective data controllers would then have to individually approach all users and ask for their prior express consent for this new purpose of their personal data processing.

Purpose limitation goes hand-in-hand with the principle of data minimisation. In order to prevent unnecessary and potentially unlawful data processing, app developers must carefully consider which data are strictly necessary to perform the desired functionality.

Third parties obtaining access to the user data through the apps must respect the principles of purpose limitation and data minimisation. Unique, often unchangeable, device identifiers should not be used for the purpose of interest based advertising and/or analytics, due to the inability of users to revoke their consent. App developers should ensure that function creep is prevented by not changing the processing from one version of an app to another without giving the end users appropriate information notices and opportunities to withdraw from either the processing or the entire service. Users should also be offered the technical means to verify statements about declared purposes, by allowing them access to information about the amounts of outgoing traffic per app, in relation to user-initiated traffic.

Information and user controls are the key features to ensure the respect of the principles of data minimisation and purpose limitation.

Control over the access to data stored in the device relies on different mechanisms:

a) OS and device manufacturers and app stores define rules that apply to submit apps in their app store: app developers must respect these rules.
b) Operating Systems' APIs define standard methods to access the data stored in the telephone to which apps have access. They also have an impact on the collection of data on the server side.
c) Ex-ante controls-controls in place before installing an app.
d) Ex-post controls-controls implemented after having installed an app.

Security

According to section 27 of the DPA, data controllers and processors must take the necessary organisational and technical measures to ensure the protection of the personal data they process. As a result, measures have to be taken by all actors, each according to their role and responsibility. In order to comply with their respective security obligations as data controllers, app developers, app stores, OS and device manufacturers and third parties have to take the principles of privacy by design and by default into account. This requires an ongoing assessment of both existing and future data protection risks, and implementation and evaluation of effective mitigating measures, including data minimisation. Good practices which can be put in place during the design of an app include that of minimising the lines and complexity of code, and implementing checks to exclude that data might be unintentionally transferred or compromised. In addition, all inputs should be validated to prevent buffer overflow or injection attacks. Other security mechanisms which are worth mentioning include adequate security patch management strategies and performing regular, independent system security audits. Additionally, app design criteria should include the implementation of the principle of the least privileged by default, whereby apps are enabled to access only the data they really need to make a functionality available to the user. App developers and app stores should also encourage users, with warnings, to complement these good design practices by virtuous user practices, such as updating their apps to the latest available versions, and reminders to avoid the reuse of passwords across different services. During the design stage of the app, app developers must also take measures to prevent unauthorised access to personal data by ensuring that data are protected both in transit and when stored, when applicable.

Mobile apps should run in specific locations within the memory of the devices (sandboxes which is a security mechanism to separate running programs.), in order to reduce the consequences of malware/malicious apps. In close collaboration with the OS manufacturer and/or app store, app developers must use available mechanisms that allow users to see what data are being processed by which apps, and to selectively enable and disable permissions. The use of hidden functionalities should not be allowed.

App developers must carefully consider their methods of user identification and authentication. They should not use persistent (device-specific) identifiers, but, instead, use low entropy app-specific or temporary device identifiers to avoid tracking users over time. Privacy-friendly authentication mechanisms should be considered. When authenticating users, app developers must give special care to the management of user-ids and passwords. The latter must be stored encrypted and securely, as a keyed cryptographic hash value. Making a test available to users on the robustness of chosen passwords is also a useful technique to encourage better passwords (entropy check). When appropriate (access to sensitive data, but also access to paid-for resources) re-authentication could be envisaged, also by means of multiple factors and different channels (e.g. access code sent by SMS) and/or the use of authentication data linked to the end user (rather than to the device). Also, when selecting session identifiers, unpredictable strings should be used possibly in combination with contextual information such as date and time, but also include IP address or geo-location data. There is also the need to have and continuously evaluate a thorough “security plan”

covering the collection, storage and processing of any personal data, to prevent such breaches from occurring. The security plan, among others, must also provide for vulnerability management and for timely and secure release of reliable bug fixes. The responsibility of app developers for the security of their products does not end with the delivery of a working version to the market. Apps may, as any software product, suffer from security flaws and vulnerabilities and app developers must develop fixes or patches for these and provide them to those players that can make them available to the users or do it themselves.

The goal of compliance with the security obligation is twofold. It will empower users to more stringently control their data, and enhance the level of trust in the entities that actually handle users' data.

App stores are an important intermediary between end users and app developers and should include a number of robust and effective checks on apps before admitting them to the marketplace. They should provide information on the checks they are actually performing, and include information on what type of data protection compliance checks they carry out.

While this measure is not 100% effective in eliminating the dissemination of malicious apps, statistics show that this practice greatly reduces the occurrence of malicious functionalities in "official" app stores. In order to cope with the large number of apps that are submitted on a daily basis this process might benefit from the availability of automatic analysis tools as well as from implementing information exchange channels between security experts and software professionals and effective procedures and policies to deal with reported issues.

In addition to the review of apps before admittance to the app store, apps should also be subjected to a public reputation mechanism. Apps should not just be rated by users for how "cool" they are, but also on the basis of their functionalities, with specific reference to privacy and security mechanisms. Also, reputation mechanisms should be engineered to prevent false ratings. Qualification and reputation mechanisms for apps can also prove effective in building mutual trust between the various entities, especially if data are exchanged through a long chain of third parties.

How Mobile Apps Are under Attack?

A research made by Arxan Technologies has shown that mobile apps are being attacked by hackers from:

- tampering,
- piracy,
- IP theft, and
- Malware /exploit injection attacks.

The above research shows that:

1. More than 90% of top paid mobile apps have been hacked which consist of:
    a. 92% of Top 100 paid apps for Apple iOS and
    b. 100% of Top 100 paid apps for Android.

2. Free apps are easily hacked which consist of:
    a. 40% of popular free Apple iOS apps and
    b. 80% of the same free Android apps.

3. Hacking is inevitable across all categories of mobile apps.
   The research has shown that hacked versions of apps were found across all key industries such as:
   - games,
   - business,
   - productivity,
   - financial services,
   - social networking,
   - entertainment,
   - communication, and
   - health

4. Mobile apps are subject to many diverse types of hacks and tampering attacks such as:
   - disabled or circumvented security,
   - unlocked or modified features,
   - free pirated copies,
   - ad-removed versions,
   - source code/IP theft, and
   - illegal malware-infested versions.

5. Financial risks from hacking are increasing rapidly as:
   Mobile app hacking is becoming a major economic issue with consumer and enterprise mobile app revenues growing to over $60 billion and mobile payments volume exceeding $1 trillion by 2016.

6. "Anatomy of an App Hack" involves three steps:
   - 1. Define the exploit and attack targets,
   - 2. Reverse-engineer the code, and
   - 3. Tamper with the code - this process is made easy with widely available free or low-cost hacking tools.

7. Traditional approaches to app security (e.g., secure software development practices, app vulnerability scanning) do not protect against these new attack vectors, leaving app owners unprepared against hackers.

8. Most app owners have not yet taken adequate measures to protect their apps against these attacks:

as an estimate, less than 5% of popular apps contain professional-grade protections to defend against hacking attacks.

Hacking Attacks faced by Mobile Apps

Hackers/Crackers most of the time makes use of the following scenarios to trigger attacks: or

1. Deactivate or By-pass security source code
2. Install Free Pirated copies of Apps containing malwares
3. Unlock or alter features to spy personal data
4. Malware Injection in the apps
5. Using weaknesses found in open source code apps provide vulnerabilities to attackers

Parties

App Stores:-

App stores often have implemented a method to remotely uninstall malicious or insecure apps. This mechanism, if not properly designed, might constitute a hindrance to empowering users to keep tighter control of their data. A privacy- friendly means for an app store to remotely uninstall apps should therefore be based on information and user consent. Moreover, from a more practical standpoint, feedback channels should be given to users to report security problems with their apps and on the effectiveness of any remote removal procedure.

Operating Systems (OS) and device manufacturers:-

OS and device manufacturers are also an important player in the definition of minimum standards and best practice amongst app developers, not only in the security of the underlying software and APIs but also in the tools, guidance and reference material they make available. OS and device manufacturers should make available strong and well known encryption algorithms and support appropriate key lengths. They should also make strong and secure authentication mechanisms available for app developers (e.g. the use of certificates signed by trusted certification authorities to verify the authorization of a remote resource). This would also avoid the need for app developers to develop proprietary authentication mechanisms. In practice this is often poorly implemented and may represent a serious vulnerability.

The access to and processing of personal data by apps should be managed through API built-in classes and methods providing proper checks and safeguards. The OS and device manufacturers should ensure that methods and functions allowing access to personal data include features aiming to implement granular consent requests. Similarly, action should be taken in order to exclude or limit access to personal data by using low-level functions or other means that could circumvent controls and safeguards incorporated into APIs.

OS and device manufacturers must also develop clear audit trails into the devices such that end users can clearly see which apps have been accessing data on their devices. All parties must respond quickly to security vulnerabilities in a timely fashion such that end users are not unnecessarily exposed to security flaws. OS and device manufacturers, together with app developers, must provide end users with upfront information about the length of time they might expect regular security updates. They should also inform users as soon as possible if a security issue requires an update to fix.

THIRD PARTIES:-

The above security features and considerations must also be applied by third parties when they collect and process personal data for their own purposes, foremost advertisers and analytics providers. This includes secure transmission and encrypted storage of unique device and app user identifiers and other personal data.

The obligation to inform and the content required

According to section 22 of the DPA, each data subject has a right to know the identity of the data controller who is processing their personal data. Additionally, in the context of apps, the end user has the right to know what type of personal data is being processed and for what purpose/s the data is/are intended to be used. If the personal data of the user are collected from other actors in the app ecosystem, the end user has the right to be informed about such data processing. Therefore, if processing personal data the relevant data controller must inform potential users at the minimum about:

- who they are (identity and contact detail),
- the precise categories of personal data the app developer will collect and process,
- why (for what precise purposes),
- whether data will be disclosed to third parties
- how users may exercise their rights, in terms of withdrawal of consent and deletion of data.

Availability of this information on personal data processing is critical in order to obtain consent from the user for the data processing. Consent can only be valid if the person has first been informed about the key elements of the data processing. Providing such information only after the app has started to process personal data (which often starts during installation) is not deemed sufficient and is legally invalid. Adequate information is also of vital importance when the app processes special categories of personal data, e. g. on health condition, political beliefs, sexual orientation, etc. Finally, the app developer should clearly differentiate mandatory and optional information and the system should allow the user to refuse access to optional information using privacy friendly default options.

With regard to the identity of the data controller, users need to know who is legally responsible for the processing of their personal data and how that controller can be contacted. Otherwise they cannot exercise their rights, such as the right to access data (remotely) stored about them. Due to the fragmented nature of the app landscape, it is crucial that every app has a single point of contact, taking responsibility for all the data processing that takes place via the app. It must not be left to the end user to research the relations between app developers and other parties processing personal data through the app.

With regard to the purpose(s), end users must be adequately informed which data are collected about them and why. Users should also be made aware in clear and plain language whether the data may be reused by other parties, and if so, for what purposes. Elastic purposes such as ‘product innovation’ are inadequate to inform users. It should be plainly stated if users will be asked to consent to data sharing with third parties for advertising and/or analytics purposes. There is an important responsibility for the app stores to ensure that this information is available and easily accessible for each app.
There is an important responsibility for app stores to ensure appropriate information. The use of visual signifiers or icons regarding data uses is strongly recommended to make users aware of the types of data processing.

Data controllers should be able to provide to the users information on:

- proportionality considerations for the types of data collected or accessed on the device,
- retention periods of the data,
- security measures applied by the data controller
- Privacy policies should also include information on how the DPA is being complied with.

The essential scope of information about data processing must be available to the users before app installation, via the app store. Secondly, the relevant information about the data processing must also be accessible from within the app, after installation.
As a joint controller with the app developers with regard to information, app stores must ensure that every app provides the essential information on personal data processing. They should check the hyperlinks to included pages with privacy information and remove apps with broken links or otherwise inaccessible information about the data processing.

Information about personal data processing should be available, and easy to locate, such as within the app store and preferably on the regular websites of the app developer responsible for the app. It is unacceptable that the users be placed in a position where they would have to search the web for information on the app data processing policies instead of being informed directly by the app developer or other data controller.

At the very least, every app should have a readable, understandable and easily accessible privacy policy, where all the above mentioned information is included. Many apps do not meet this minimum transparency requirement. Apps which do not, or are not intended for the processing or personal data, should clearly state this within the privacy policy.

Further information is available through links to the whole privacy policy. The information should be presented directly on screen, easily accessible and highly visible. Next to comprehensive information suitable for the small screen of mobile devices, users must be able to link through to more extensive explanations, for example in the privacy policy, how the app uses personal data, who the data controller is and where a user can exercise his rights.

This approach may be combined with the use of icons, images, video and audio, and make use of contextual real time notification when an app accesses the address book or photos. These icons have to be meaningful, i.e. clear, self-explaining and unambiguous. Clearly, the OS manufacturer has an important joint responsibility to facilitate the use of such icons.

Additionally, users should always be provided with the possibility to withdraw their consent in a manner which is simple and not burdensome. A data subject may withdraw consent for data processing in a number of different ways and for a number of different reasons. Preferably the option of consent withdrawal should be available through the above mentioned easily accessible mechanisms. It must be possible to un-install apps and thereby remove all personal data, also from the servers of the data

controller(s). In order to allow users to have their data deleted by the app developer, there is an important role for the OS manufacturer to provide a signal to the app developer once a user uninstalls the app. Such a signal could be provided through the API. In principle, after the user has uninstalled the app, the app developer does not have a legal ground to continue processing of the personal data relating to that user, and therefore has to delete all data. An app developer that wishes to keep certain data, for example in order to facilitate reinstallation of the app, has to separately ask for consent in the uninstalled process, asking the user to agree to a defined extra retention period. The only exception to this rule is the possible existence of legal obligations to retain some data for specific purposes, for example fiscal obligations relating to financial transactions.

Retention periods

App developers must consider the retention of data collected with the app and the data protection risks these pose. The specific timescales will depend on the purpose of the app and the relevance of the data to the end user. For example, a calendar, diary or photo sharing application would place the retention schedule into the control of the end user where for a navigation app it may suffice to store only the last 10 recently visited locations. App developers should also give consideration to the data of those users who have not used the app for an extended period of time. These users may have lost their mobile device, or switched to another device without actively uninstalling all apps on the initial device. App developers should therefore predefine a time period of inactivity, after which the account will be treated as expired and ensure that the user is informed of such a timescale. Upon expiry of this time period, the data controller should alert the user and give the user a chance to retrieve personal data. If the user doesn't respond to the alert, personal data relating to the user and usage of the app should be irreversibly anonymised or deleted. The reminder period depends on the purpose of the app and the location where the data are stored. If it concerns data stored on the device itself, for instance a high score in a game, the data may be kept as long as the app is installed. If it concerns data that are only used once per year, such as information on a touristic resort, the reminder period could be 15 months.

Recommendations

1. App developers must take the necessary organisational and technical measures to ensure the protection of the personal data they process, at all stages of the design and implementation of the app (privacy by design).

2. The operating system of mobile devices using apps that process sensitive information assets must be hardened against binary-level integrity or reverse-engineering attacks before putting it on market.

3. Apps devices must provide a transparent operating system which would provide tracks to the user for any hidden apps containing malware or spyware. This will prevent any malicious or spy apps to run into the mobile hidden environment device without the consent or knowledge of the user at the backend.

4. Make provision to construct counter-security protections directly into all the apps to:
   a) Assess risks and attack targets in the apps,
   b) Harden the code against reverse-engineering, and
   c) Make the apps tamper-proof and self-defending.

5. Incorporate the mobile apps protection as default to allow innovation and distribute high-value and sensitive mobile apps.

6. Manufacturer of apps must make provision for a guaranteed automatic lifetime update of patches into the operating system of mobile devices or provide an option for update of new release of operating system which would be able to remove any malicious apps such as malware and spyware.

7. Manufacturers of mobile device must provide the option of an administrator mode and limited access mode in the operating system. The administrative mode will be used only to install apps and for maintenance purpose. The limited mode will be used for all other functionality with limited access such as surfing to internet which will prevent any malicious apps to access and modify via backdoors.

8. Manufacturers of mobile device must make provision to enable whitelisting mode which is a control that permits only known safe apps to execute commands.

9. Manufacturers of mobile device must prioritise security protections for mobile apps that deal with transactions payments, sensitive data or any high-value profile.

10. The manufacturer of mobile device must provide a much secured mode of two-factor authentication especially for conducting sensitive transactions on mobile devices. Two-factor refers to an authentication system in which users are required to authenticate using at least two different “factors” something you know, something you have, or something you are before being granted access.

11. Manufacturers of mobile apps must provide a secured mode of transmission, that is, an encrypted mode for email or any other types of data communication in order to prevent any unintended interception by hacker or cracker.

12. Manufacturers of mobile device must provide a mandatorily secured anti malware environment such as preinstalled antivirus and firewall apps to protect against malicious applications, trojans, spams, viruses, spyware, and malware-based attacks which will prevent users into revealing passwords or other confidential information.

13. Manufacturers of mobile device must not prompt the user for connection to an unsecured WiFi network which will allow an attacker to access personal information from a device, putting users at their own risk for data and identity theft such as the man-in-the-middle, where an attacker inserts himself in the middle of the communication stream and steals information. Having communication channels, such as Bluetooth communications, "open" or in "discovery" mode could allow an attacker to install malware through that connection, or secretly activate a microphone or camera to eavesdrop on the user. In addition, using unsecured public wireless Internet networks or WiFi spots could allow an attacker to connect to the device and view sensitive information.

14. Manufacturers of mobile device must provide the necessary apps to detect for remotely disabled lost or stolen devices as a feature for lost or stolen devices that either locks the device or completely erases its contents by the administrator/ owner by remote access which can only be unlocked subsequently by the user if they are recovered.

15. Manufacturers of mobile apps must provide a mobile apps' security policy to define the rules, principles, and practices that determine how an organisation treats mobile devices, whether they are issued by the organisation or owned by individuals. Policies should cover areas such as roles and responsibilities, infrastructure security, device security, and security assessments. By establishing policies that address these areas, users can create a framework for applying practices, tools, and training to help support the security of wireless networks.

App developers must further:-

- comply with their obligations as data controllers when they process data from and about users;

- comply with their obligations as data controllers when they contract with data processors such as if they outsource the collection and processing of personal data to developers, programmers and for example cloud storage providers;

- Ask for consent before the app starts to retrieve or place information on the device, i.e., before installation of the app. Such consent has to be freely given, specific and informed;
- Ask for granular consent for each type of data the app will access; at least for the categories Location, Contacts, Unique Device Identifier, Identity of the data subject, Identity of the phone, Credit card and payment data, Telephony and SMS, Browsing history, Email, Social networks credentials and Biometrics;
- Be aware that consent does not legitimise excessive or disproportionate data processing;
- Provide well-defined and comprehensible purposes of the data processing in advance to installation of the app, and not change these purposes without renewed consent; provide comprehensive information if the data will be used for third party purposes, such as advertising or analytics;
- Allow users to revoke their consent and uninstall the app, and delete data where appropriate;
- Respect the principle of data minimisation and only collect those data that are strictly necessary to perform the desired functionality;
- Provide a single point of contact for the users of the app;
- Provide a readable, understandable and easily accessible privacy policy, which at a minimum informs users about:
- who they are (identity and contact details),
- what precise categories of personal data the app wants to collect and process,
- why the data processing is necessary(for what precise purposes),
- whether data will be disclosed to third parties (not just a generic but a specific description to whom the data will be disclosed),
- what rights users have, in terms of withdrawal of consent and deletion of data;
- Enable app users to exercise their rights of access, rectification, erasure and their right to object to data processing and inform them about the existence of these mechanisms;
- Define a reasonable retention period for data collected with the app and predefine a period of inactivity after which the account will be treated as expired;
- With regard to apps aimed at children: pay attention to the age limit defining children or minors in local laws, choose the most restrictive data processing

approach in full respect of the principles of data minimisation and purpose limitation, refrain from processing children's data for behavioural advertising purposes, either directly or indirectly and refrain from collecting data through the children about their relatives and/or friends.

- Proactively inform users about personal data breaches;
- Inform users about their proportionality considerations for the types of data collected or accessed on the device, the retention periods of the data and the applied security measures;
- Develop tools to enable users to customise retention periods for their personal data based on their specific preferences and contexts, rather than offering pre-defined retention terms;
- Include information in their privacy policy dedicated to users;
- Develop and implement simple but secure online access tools for users, without collecting additional excessive personal data;
- Together with the OS and device manufacturers and app stores use their creative talent to develop innovative solutions to adequately inform users on mobile devices, for example through a system of layered information notices combined with meaningful icons.

App stores must:-

- comply with their obligations as data controllers when they process data from and about users;
- Enforce the information obligation of the app developer, including the types of data the app is able to access and for what purposes, as well as whether the data is shared with third parties;
- Give special attention to apps directed at children to protect against the unlawful processing of their data, and especially enforce the obligation to present the relevant information in a simple manner, in age specific language;
- Provide detailed information on the app submission checks they actually perform, including those aimed to assess privacy and data protection issues.
- In collaboration with the OS manufacturer, develop control tools for users, such as symbols representing access to data on and generated by the mobile device;
- Subject all apps to a public reputation mechanism;
- Implement a privacy friendly remote uninstall mechanism;

- Provide feedback channels to users to report privacy and/or security problems;
- Collaborate with app developers to pro-actively inform users about personal data breaches;
- Warn app developers about the specificities of the DPA before submitting the application in Mauritius, for example about the consent requirement and in case of transfers of personal data abroad.

OS and device manufacturers must:-

- Update their APIs, store rules and user interfaces to offer users sufficient control to exercise valid consent over the data processed by apps;
- Implement consent collection mechanisms in their OS at the first launch of the app or the first time the app attempts to access one of the categories of data that have significant impact on privacy;
- Employ privacy by design principles to prevent secret monitoring of the user;
- Ensure security of processing;
- Ensure (the default settings of) pre-installed apps are compliant with data protection laws;
- Offer granular access to data, sensors and services, in order to ensure that the app developer can only access those data that are necessary for his app;
- Provide user-friendly and effective means to avoid being tracked by advertisers and any other third party. The default settings must be such as to avoid any tracking;
- Ensure the availability of appropriate mechanisms to inform and educate the end user about what the apps can do and what data they are able to access;
- Ensure that each access to a category of data is reflected in the information of the user before the app's installation: the categories presented must be clear and comprehensible;
- Implement a security-friendly environment, with tools to prevent malicious apps from spreading and allow each functionality to be installed/uninstalled easily;
- Enable users to uninstall apps, and provide a signal (for example through the API) to the app developer to enable deletion of the relevant user data;

- Systematically offer and facilitate regular security updates;
- Ensure that methods and functions allowing access to personal data include features aiming to implement granular consent requests;
- Actively help develop and facilitate icons alerting users to different data usage by apps;
- Develop clear audit trails into the devices such that end users can clearly see which apps have been accessing data on their devices and the amounts of outgoing traffic per app, in relation to user-initiated traffic.

Third parties must:-

- Comply with their obligations as data controllers when they process personal data about users;
- Comply with the consent requirement determined in section 2 of the DPA when they read or write data on mobile devices, in cooperation with the app developers and/or app stores, which essentially provide user with the information on the purposes of data processing;
- Not circumvent any mechanism designed to avoid tracking, as it currently often happens with the "Do Not Track" mechanisms implemented in browsers;
- Communications service providers, when they issue branded devices, must ensure the valid consent of users for pre-installed apps and take on board relevant responsibilities when contributing to determining certain features of the device and of the OS, e.g. when limiting the user's access to certain configuration parameters or filtering fix releases (security and functional ones) provided by the device and OS manufacturers;
- Advertising parties must specifically avoid delivering ads outside the context of the app. Examples are delivering ads by modifying browser settings or placing icons on the mobile desktop. Refrain from the use of unique device or subscriber identifiers for the purpose of tracking;
- Refrain from processing children's data for behavioural advertising purposes, either directly or indirectly. Apply appropriate security measures. This includes secure transmission and encrypted storage of unique device and app user identifiers and other personal data.
- Develop and implement simple but secure online access tools for users, without collecting additional excessive personal data;
- Only collect and process data that are consistent with the context where the user provides the data.

References:

http://www.arxan.com/assets/1/7/state-of-security-app-economy.pdf
(date accessed 24 July 2014)

https://www.arxan.com/assets/1/7/State_of_Security_in_the_App_Economy_Report_Vol._2.pdf(date accessed 24 July 2014)

Warsaw declaration on the ''appification" of society (24 September 2013)