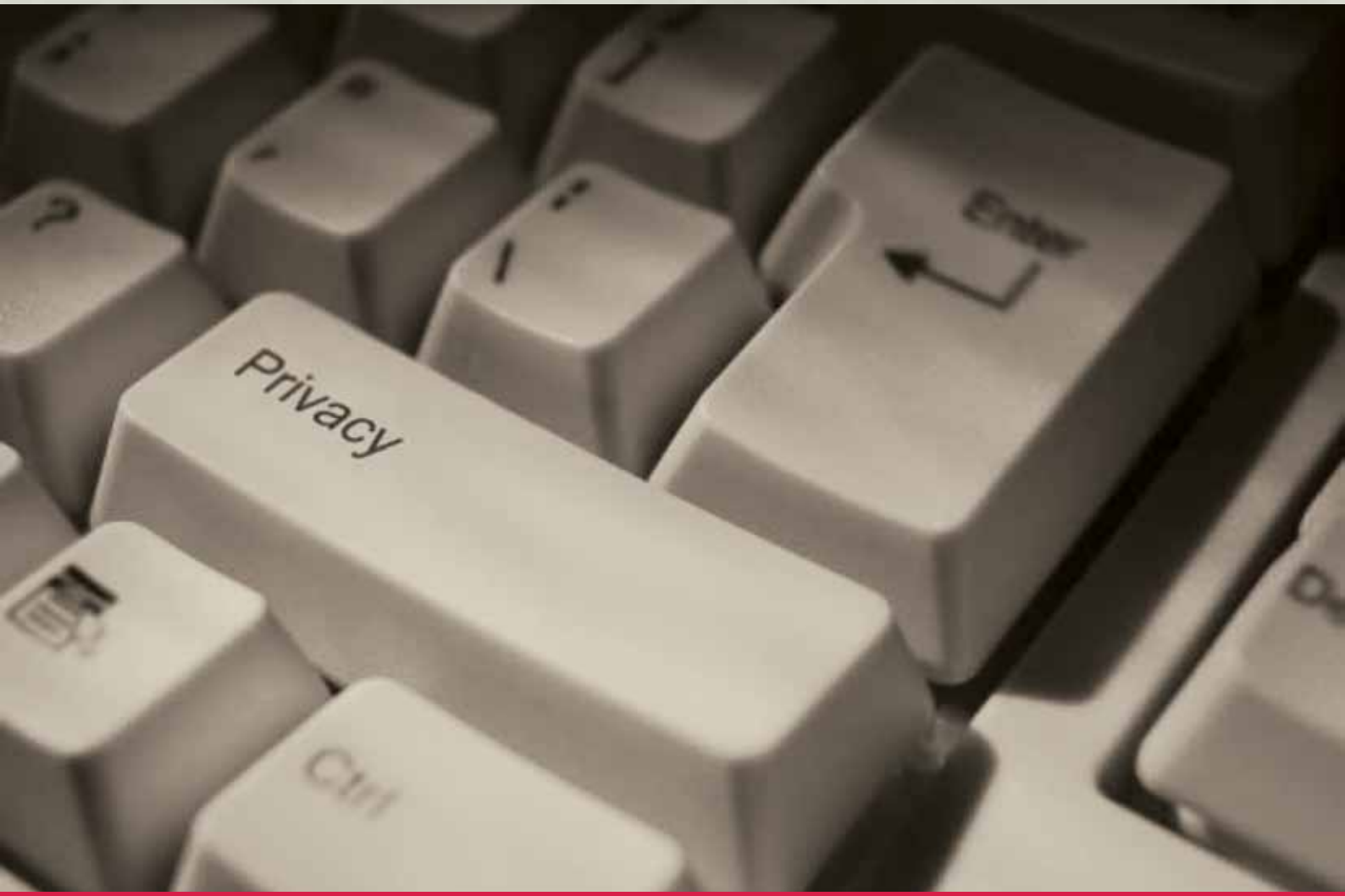
DPO
Data Protection Office

PRIVACY ENHANCING TECHNOLOGIES

An Absolute Necessity for Effective Compliance with Data Protection Laws

Volume 7



Guidance issued by the ***Data Protection Commissioner*** to assist data controllers and processors in implementing privacy enhancing technologies

PRIVACY ENHANCING TECHNOLOGIES

An Absolute Necessity for Effective Compliance with Data Protection Laws

Volume 7

Mrs Drudeisha Madhub
Data Protection Commissioner
Tel.: 201 3604
Helpdesk: 203 9076
Email: pmo-dpo@mail.gov.mu
Website: http://dataprotection.gov.mu

TABLE OF CONTENTS

INTRODUCTION

The use of the internet and email to communicate, research areas of interest and interact with businesses and government is at all time high driven by a strong uptake of broadband services in Mauritius and worldwide. There is a growing tendency towards introducing more computing power and/or information storage in our everyday activities, which is redefining how we interact with our environment and potentially generating information about our opinions, preferences and lifestyles, but hidden to us. Cloud computing and data centers have revolutionised the industrial world but has data protection implications which should be seriously looked into by all stakeholders to avoid putting people's privacy rights at stake. The solution to all privacy problems are the adoption of appropriate privacy enhancing technologies.

WHAT ARE PRIVACY ENHANCING TECHNOLOGIES?

Technology can assist data controllers' compliance with data protection principles and can go further to empower individuals, giving them easier access to and control over information about them and allowing them to decide how and when these information will be disclosed to and used by third parties.

The best protection for individuals is when their personal information is only collected when required. Privacy enhancing technologies have traditionally been limited to 'pseudonymisation tools' which are software and systems that allow individuals to withhold their true identity from those operating electronic systems or providing services through them, and only reveal it when absolutely necessary. These technologies help to minimise the information collected about individuals and include anonymous web browsers, specialist email services, and digital cash.

For instance, recognised identity management systems potentially allow individuals to access the services of organisations without having to provide information to them. They involve one trusted organisation verifying the identity of an individual and then vouching for them using an electronic token that also specifies their particular entitlements. This allows the individual to access the services provided by third parties using the token without having to disclose their identity or other information necessary to prove their entitlement.

Privacy enhancing technologies should however not be limited to tools that provide a degree of anonymity to living individuals as they should include any technology that protects or enhances an individual's privacy, including facilitating individuals' access to their rights under the Data Protection Act 2004.

Examples of this wider approach to privacy enhancing technologies could include:

- encrypted biometric access systems that allow the use of a fingerprint to authenticate an individual's identity, but do not retain the actual fingerprint;

- secure online access for individuals to their own personal data to check its accuracy and make amendments;

- software that allows browsers to automatically detect the privacy policy of websites and compares it to the preferences expressed by the user, highlighting any clashes; and 'sticky' electronic privacy policies that are attached to the information itself preventing it being used in any way that is not compatible with that policy.

WHY USE PRIVACY ENHANCING TECHNOLOGIES?

Cost-effectiveness

The cost of including privacy at the system design stage is much less than the cost of having to amend a finished system to make sure it complies with legal requirements and respects individuals' privacy.

Risk Mitigator

Privacy controls that are incorporated into electronic information systems to supplement organisational procedures help to provide additional safeguards which better protect individuals' information from human error.

Building Trust

The use of privacy enhancing technology in systems helps to signal the integrity and intention of organisations regarding the information that they hold, and encourages trust in those organisations by citizens and customers.

Engineering privacy/data protection compliance

A system designer who starts from the position of trying to protect individuals' privacy by creating or implementing privacy enhancing technologies might ask the following questions as an essential part of the task:-

- Do I need to collect any personal data at all?
- If so, what is the minimum needed?
- Who will have access to which data?
- How can access be controlled to allow only those employees and processes that have an essential need?
- Can individuals make total or partial use of the system anonymously?
- How can I help individuals to exercise their rights securely?

The Data Protection Commissioner encourages the software and hardware industry to work on internet privacy-compliant products that provide the necessary tools to comply with the data protection rules contained in the Data Protection Act.

A condition for legitimate processing of personal data is the requirement that the data subject is informed and thus made aware of the processing in question. Therefore, this office is especially concerned about all kinds of processing operations which are presently being performed by software and hardware on the Internet without the knowledge of the person concerned and which are "invisible" to him/her.

Typical examples of such invisible processing are the "chattering" at the HTTP level, automatic hyperlinks to third parties, active content (like Java, ActiveX or other client based scripting technologies) and the cookies mechanism as currently implemented in the common browsers[1].

Internet software and hardware products should provide the Internet users information about the data that they intend to collect, store or transmit and the purpose for which they are necessary.

Internet software and hardware products should also give the capacity to the data user to easily access any data collected about him/her at any later stage.

In the case of browser software for example, on establishing a connection with a web server (sending a request or receiving a Web page), the user must be informed of which information is intended to be transferred and for what purposes.

In the case of hyperlinks sent by a web site to a user by whatever means, the browser software should reveal them to the user.

In the case of cookies, the user should be informed when a cookie is intended to be received, stored or sent by the Internet Software. The message should specify, in generally understandable language, which information is intended to be stored in the cookie, for what purpose as well as the period of validity of the cookie.

---

1 An example of this type of technique is the so-called cookie, which can be defined as a computer record of information that is sent from a web server to an user's computer for the purpose of future identification of that computer on future visits to the same web site.

Browsers are software programs designed to, among other things, graphically display material that is available on the Internet. Browsers communicate between the user's computer (client) and the remote computer where information is stored (Web server).

Browsers often send more information to the Web server than strictly necessary for establishing the communication. Classical browsers will automatically send to the Web server visited the type and language of the browser, the name of other software programmes installed on the user's PC and operating system, the referring page, cookies etc. Such data can also be transmitted systematically to third parties by the browser software, in an invisible way.

These techniques allow the creation of clicktrails about the Internet user. Clicktrails consist of information about an individual's behaviour, identity, pathway or choices expressed while visiting a web site. They contain the links that a user has followed and are logged in the web server.

The Data Protection Act contains detailed provisions for the protection of individuals with regard to the protection of personal data. Cookies or browsers can contain or further process data allowing the direct or indirect identification of the individual Internet user.

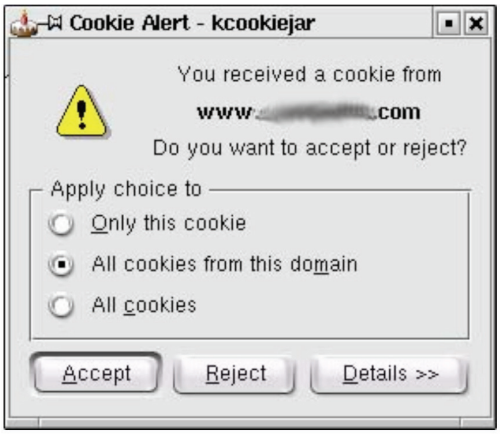
The configuration of hard- and software products should not, **by default**, allow for collecting, storing or sending of client persistent information. For example: Browser software should, **by default**, be configured in such a way that only the minimum amount of information necessary for establishing an Internet connection is processed. Cookies should, **by default**, not be sent or stored.

During its installation, a browser's feature designed to store and send data about user's identity or communication behaviour (profile) should not be filled in automatically with any data previously stored on the user's equipment.

Internet hard and software products should allow the data subject to freely decide about the processing of his/her personal data by offering user-friendly tools to filter (i.e. to reject or to modify) the reception, storage or sending of client persistent information following certain criteria (including profiles, the domain or the identity of the Internet server, the kind and the duration of the information being collected, stored or sent and so on).

The user should be provided with clear instructions regarding the use of soft and hardware for the implementation of these options and tools. For example: the browser software should provide options so that the user can configure the browser, specifying which information the browser should or should not collect and transmit.

For cookies, the user should always be given the option to accept or reject the sending or storage of a cookie as a whole. Also the user should be given options to determine which pieces of information should be kept or removed from a cookie, depending on e.g. the period of validity of the cookie or the sending and receiving Web sites.



Internet software and hardware products should allow the users to remove client persistent information in a simple way and without involving the sender. The user should be given clear instructions on how to do this. If the information cannot be removed, there must be a reliable way to prevent it from being transferred and read.[2]

Cookies and other client persistent information should be stored in a standardised way and be easily and selectively erasable at the client's computer (Please consult the guidelines volume 8 issued by this office on this particular subject).

Presently it is almost impossible to use the Internet without being confronted with privacy invading features which carry out all kinds of processing operations of personal data in a way that is invisible to the data subject. In other words, the Internet user is not aware of the fact that his/her personal data have been collected and further processed and might be used for purposes that are unknown to him/her. The data subject does not know about the processing and has no freedom to decide on it.

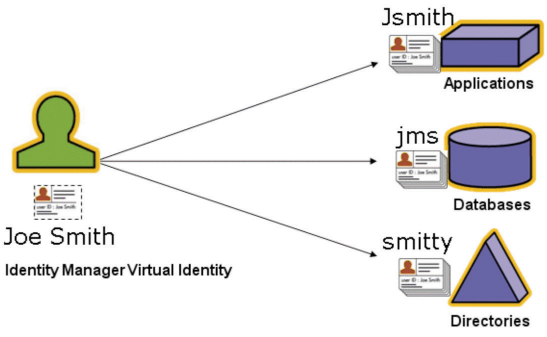
BACKGROUND AND FUTURE PERSPECTIVES FOR TRUSTED COMPUTING PLATFORMS

This concept is increasing in importance as forecasts of Internet use predict a decline in the relative importance of the Web – the public part of the Internet characterised by a large number of unsecured transactions – with private areas where security concerns will be paramount.

As the foundations of security are perpetually under construction, electronic/digital signatures and their legal development are attempts to deal with issues raised by transactions on the network, while trusted computing platforms are intended to deal with issues related to the ownership, integrity and, where necessary, confidentiality of intangible goods, and to controlling their use in terms of both software and hardware. Not all of the various building blocks of these new, highly sophisticated architectures have yet matured enough to certify the highest level of security whilst using them.

Past attempts to increase security by identifying hardware components (such as Intel's Pentium III, which included a unique universal identifier) faced setbacks because of the risks to privacy. Researchers are now turning to sophisticated cryptology techniques, with a focus on protection of privacy and personal data. For this reason, PETs (privacy enhancing technologies) applications such as individual digital safes or virtual identity managers have been proposed for trusted computing platforms.

The roles of users and administrators should be clearly differentiated. It is administrators who are responsible for defining and limiting both the technical and practical rights of the users. Computing platforms capable of administering these rights would be trusted computing platforms.



Security chips[3] have been developed and are targeted to everyday computing, and so, the focus of industry efforts is on securing hardware platforms.

The development of specific applications are, for example, applications such as Digital Rights Management (DRM), the Next Generation Secure Computing Base (formerly known as Palladium) by Microsoft and the Intel La Grande technology.

Both those who design technical specifications and those who actually build or implement applications or operating systems bear responsibility for the data protection aspects, although at different levels. Those who build, commercialise and use the applications bear responsibilities as well, especially organisations that process user data, as they will normally be the last one in the chain and the ones who interact with the user.

Many of the principles of the Data Protection Act have significant implications in this context. The Commissioner would particularly like to emphasise the importance of the principles of proportionality and of the justification to collect and process the data. These principles imply that, in striking a balance between the fundamental rights of data subjects and the interests of the different actors involved, as few personal data as possible should be processed.

These principles have implications on the design of the new protocols and devices: while technology is *per se* neutral, applications and design of new technological tools should be privacy compliant *by default*.

3 A security chip has the following functionalities:
public key functions: key pair generation, public key signature, verification, encryption and decryption;
trusted boot functions: Platform Configuration Registers (PCR) store hashes of configuration information throughout the boot sequence. Once booted, data (such as symmetric keys for encrypted files) can be "sealed" under a PCR initialisation and management functions: allowing the owner to turn functionality on and off, reset the chip, and take ownership. The new version of the specifications allows the owner to delegate a number of the functions to the user.

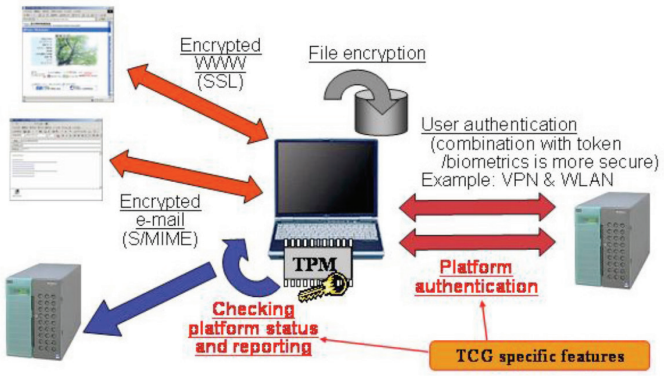
GENERAL OBSERVATIONS ON THE BASIC GUIDELINES CURRENTLY ACCEPTED ACROSS THE INDUSTRY

Informing users

In practice, the technical complexity of trusted computing-mechanism systems makes it difficult to assume that the average user will be able to understand the information about the system and make informed choices as to their use. Simple and understandable information must be provided to users and, even more important, to make sure that sufficient protection is provided in all cases.

Security features

The trusted computing mechanisms specifications include features that reinforce security. It is further recommended wherever possible for the level of security to be "tuned" to specific uses of the system on a case-by-case basis. After all, security should be proportional to the risks at stake and these risks will vary depending on the situation: for instance, when a user wants to access his medical file on-line, more security measures will be required than when an individual wants to register at a website that provides news services.



Data protection using outside certification or anonymisation

In order to limit the transmission of identifiers and also the compilation of user profiles by third parties, it should be possible for a trusted third party to certify users' identities and confirm them to their correspondents without actually revealing the identities. Concentration of data always involves additional risks and therefore sufficient precautions should be taken. As for trusted computing mechanisms, there are scenarios in which a single trusted third party controls huge amounts of authentication information.

The possibility to do without a trusted third party by using the "Direct Anonymous Attestation" (DAA) feature, which enables users to create Attestation Identity Keys (AIK) without presenting Endorsement Keys (EK), which are unique identifiers, is an improvement but the choice between the trusted third party and the DAA feature will be made by the applications.

DAA is therefore an additional possibility, not a standard feature of the system in all cases. The introduction of the DAA functionality is thus an improvement, but in the cases where it would still be possible to establish a link with the identity of the user or to create profiles of the users, there would then be no anonymity. However, the use of this functionality in the most privacy-friendly or enhancing manner should be promoted: using random identifiers as much as possible and, where revocation and identification are necessary, restricting the use of names to as short a time as possible.

The importance of the role of trust within trusted computing mechanisms systems is to be highlighted. Trust should exist through the whole chain of those involved, from the designer of specifications to the seller of applications and the deployer of the system.

Data protection should be considered at all stages of the process and format.

RADIO FREQUENCY IDENTIFICATION TECHNOLOGY

An Overview of the technology and its usages

The use of Radio Frequency Identification[4] (commonly known as "RFID technology") for different purposes and applications may benefit business, individuals and public services (governments included). RFID can help retailers manage their inventory, enhance consumers' shopping experience, improve drug safety as well as allow better control access by persons to restricted areas.

4 The basics of Radio Frequency Identification Technology:-
The simplest RFID system consists of two components: a tag, which is attached to an object, and a reader which is able to retrieve the data from the tag. These components communicate with each other via a radio link. Both tag and reader possess an antenna and a demodulator (analogue front-end). This front-end "translates" the incoming analogue information from the radio link into digital data. These data can be further processed by the digital part of the reader or the tag.

On the tag's side, digital processing can be done either by custom-designed hardware or by a microprocessor. To process the data retrieved from the tags, a host computer attached to the reader can be used. This host is required to implement special applications using the tag data.

Various technology parameters can be used to describe a particular RFID system. Depending on these parameters, different applications are possible for RFID systems.

RFID technology can work in different ways depending on the types of tags and readers. Those deploying the technology would have to choose between the different technical possibilities according to their needs. Deployers would have to decide whether to use active or passive tags.

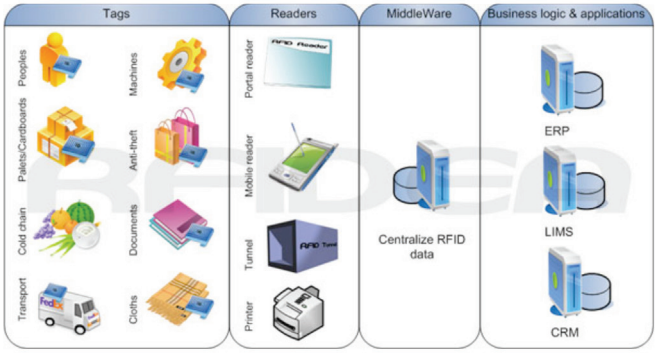
Deployers of RFID technology are required to provide data subjects with information not only on the purposes of the processing of data, but also on the presence of RFID devices as well as to comply with the following:

Firstly, individuals must be informed of the presence of RFID-like or activated RFID readers. In order to do so, pictograms in the direction of a world wide standard as well as other informational means towards that goal are an obvious need. The provision of this type of information is essential in order to prevent the unauthorised and surreptitious gathering of personal data through RFID technology. For example, if a store or hospital has activated readers, individuals should be informed about it.

Secondly, for the same reasons outlined above (avoid the surreptitious gathering of personal data) the identification of the existence of RFIDs surrounding an individual (in clothing and objects for example) is another requirement because of the RFID's size which can make it almost invisible. Methods to carry out this requirement can adopt different forms: they can be given by standard notices but also technically.

Thirdly, informing about the presence of RFID only will not suffice in practice, the activability or the real time activation of RFIDs is also a piece of information to be provided to individuals that derive from the data protection laws. So, simple techniques enabling visual indications of activation or activability states are also necessary. The presence and nature of PET technology (e.g. temporal disabler, tag physical remover feature etc.) as well as organisational measures in a given environment should be part of the information easily available.

As further described below, the way RFID technology is built may have a great impact in ensuring the effective implementation of the access, rectification and deletion rights as recognised by the Data Protection Act.



While the advantages related to the use of RFID technology seem obvious, the widespread deployment of the technology does not come without its potential drawbacks.

The possibility for some applications of RFID technology to violate human dignity as well as data protection rights is real. In particular, concerns arise about the possibility of businesses and governments to use RFID technology to pry into the privacy sphere of individuals. The ability to surreptitiously collect a variety of data all related to the same person; track individuals as they walk in public places (airport, bus stations, stores); enhance profiles through the monitoring of consumer behaviour in stores; read the details of clothes and accessories worn and medicines carried by customers are all examples of uses of RFID technology that give rise to privacy concerns. The problem is aggravated by the fact that, due to its relative low cost, this technology is not only available to major actors but also to smaller players and individual citizens.

Data Protection and Privacy Implications

Whereas some applications of RFID may not pose any data protection concerns, as illustrated below, many do.

RFID used to collect information linked to personal data

A first type of data protection concern arises when the deployment of RFID technology is used to collect information that is directly or indirectly linked to personal data. First, one can consider the case where the RFID tag number of a product is linked to the record of the customer who bought it. For example, a consumer electronics store could tag its products with unique product codes which the retailer systematically combines with customer names collected upon payment with credit cards and later on linked with the retailer customer database. This could be done for, among others, to guarantee purposes.

As a second example, one can consider the case where supermarket tags loyalty cards or similar devices which identify individuals by their names to learn and record consumer habits while consumers are in the store, including the time spent on a given section of the supermarket, the number of times the consumer visits in the supermarket without buying, etc.

In the above cases, in so far as the information gathered through RFID technology is linked to personal data, the privacy implications are obvious. In addition to enhancing the existing ability of learning consumer habits and making individual profiles enabled by loyalty cards, RFID technology increases the potential for direct marketing with item level tagging, as individuals could be recognised on entering a store and their habits in store monitored. Furthermore, widespread deployment of the technology will cause a boost in data (both in type and in number) to be processed by a wide variety of controllers, giving cause to concern.

RFID used to store personal data on each tag

A second type of privacy implication arises where personal data is stored in RFID tags. One example of this use could be in transport ticketing. One could consider the hypothetical case where an organisation decides to implement a contactless ticketing system based on RFID technology for monthly passes where the name and contact details of the holder of the pass is inserted into the tag. This would have the effect of allowing the organisation to know where an identified individual travels at all times. This obviously impacts individuals' privacy. In addition to the organisation having this information, because anyone can detect the presence of particular RFID tags with a standard reader, third parties could also surreptitiously obtain the same information. It should be noted that RFID systems are very susceptible to attacks. As they work nonline-of-sight and contactless, an attacker can work remotely and passive readings would not be noticed.

Use of RFID to track without "traditional" identifiers being available

A third type of data protection implication arises from uses of RFID technology which entail individual tracking and obtaining access to personal data. Several examples will illustrate how RFID technology may impact an individual's privacy.

For example, there is the possibility for a chain grocery store to give out tagged devices to customers (e.g., like tokens) enabling the operation of shopping carts, which customers re-use each time they visit the store. Such a mechanism would permit the store to set up a file using the identification number stored in the tagged device enabling it to monitor which products an individual (identified by the token) purchases, how often such products are used and in which of the chain grocery stores the consumer buys them. The store could make inferred assumptions about an individual's income, health, lifestyle, buying habits etc. This information could be used for various decision making, such as marketing purposes or even for dynamic pricing. Since the device would identify the individual each time he/she entered the store, the consumer could be marketed to in the light of the recorded consumer habits. In addition to the store being able to collect the above information, a third party could potentially also obtain such information. In this way, various decisions could be made about that identified individual without his or her informed consent. As it happens, with the use of cookies in the on-line environment, even if the individual is not immediately and directly identified at the item information level, he can be identified at an associative level because of the possibility of identifying him without difficulty via the large mass of information surrounding him or stored about him. Furthermore, the data collected from him can influence the way in which that person is treated or evaluated. This RFID use also carries serious data protection implications.

A further example could be where the use of RFID tags can lead to the processing of personal data, even when RFID technology does not involve the use of other explicit identifiers. Take the hypothesis where person Z walks into Shop C with a bag of RFID tagged products from Shops A & B. Shop C scans his bag and the products in it (more likely a jumble of numbers) are revealed. Shop C keeps a record of the numbers.

When person Z returns to the shop the next day, he is rescanned. Product Y, that was scanned yesterday, is revealed today – the number is for the watch he always wears. Shop C sets up a file using the number of product Y as a 'key'. This allows them to track when Person Z enters their shop, using the RFID number of his watch as

a reference number for him. This allows shop C to set up a profile of Person Z (whose name they don't know) and to track what he has in his shopping bag on subsequent visits to Shop C. By doing this, Store C is processing personal data and data protection law will apply.

Finally, take the example of the use of tags on certain objects which contain information that reveal the nature of the object. Belongings of a person are very personal and hold information whose knowledge by third parties would invade the privacy of the person who owns the object. The following examples illustrate this hypothesis. Consider the case where anyone in possession of a reader can detect banknotes, books, medicines or valuable objects of passers-by. The knowledge of this information by third parties will invade the privacy of the person who owns the object. The same concerns apply where terrorists were able to detect specific nationalities among crowds. An even more dramatic intrusion would occur when, as described above, the device itself contains important personal information as for example passport related information or information that was highly sensitive.

As illustrated in these examples, some of the main data protection and privacy concerns that arise from the use of RFID technology derive from the surreptitious, unwanted individual tracking performed by unauthorised access to the tag's disclosed information or memory content. In the three scenarios described above, the provisions of the Data Protection Act would apply. In the first case, this is because the item level information gathered through RFID technology is directly linked to personal data contained in either a credit card or loyalty cards. In the second scenario, the application of the Data Protection Act kicks in as soon as personal information such as a name is embedded in the RFID tags. Finally, the use of RFID technology to track individual movements which, given the massive data aggregation and computer memory and processing capacity are, if not identified, identifiable, also triggers the application of the Data Protection Act.

In assessing whether the collection of personal data through a specific application of RFID is covered by data protection laws, we must determine:

(a) the extent to which the data processed relates to a living individual and,

(b) whether such data concerns an individual who is identifiable or identified.

Data relates to an individual if it refers to the identity, characteristics or behaviour of an individual or if such information is used to determine or influence the way in which that person is treated or evaluated.

Those who are considering using information gathered through RFID technology before doing so will have to carry out prior assessment to determine whether such information falls within the definition of "personal data" in accordance with the Data Protection Act.

If RFID information neither contains personal information nor is combined with personal data as defined above, then the provisions of the Data Protection Act will not apply. Indeed, if tag information is not combined with other identifying material, for example someone's photograph or name and address, or with a recurring reference number, then the Data Protection Act will not apply.

Data Protection Principles

Data controllers collecting data in the context of RFID applications, must comply with several data protection principles, including the following:

The Use limitation principle (purpose principle): This principle, among others, prohibits a further processing which is incompatible with the purpose(s) of the collection.

The data quality principle: This principle requires personal data to be relevant and not excessive for the purposes for which they are collected. Thus, any irrelevant data must not be collected and if it has been collected, it must be discarded. It also requires data to be accurate and kept up-to date.

The conservation principle: This principle requires personal data to be kept for no longer than is necessary for the purpose for which the data were collected or further processed.

Legal grounds for processing

Under most of the scenarios where RFID technology is used, consent from individuals is a legal ground available to data controllers to legitimise the collection of information through RFID. For example, a supermarket that tags loyalty cards will need either explicit contractual regulations or the individual's consent to link the personal information obtained in the context of obtaining the loyalty card with information gathered through RFID technology. However, consent is not always the sole legal ground to legitimise the processing of personal data collected in the context of RFID systems. For example, a hospital that uses RFID in surgical instruments to eliminate the risk of leaving an item inside of a patient at the conclusion of an operation may not need the patient's consent insofar as this

processing might be legitimised in the vital interests of the data subject, which is another legal ground foreseen under the Data Protection Act.

Information requirements:

Data controllers processing information through RFID technology must provide the following information to data subjects: identity of the controller, the purposes of the processing as well as, amongst others, information on the recipients of the data and the existence of a right of access. In compliance with this obligation in the context of the scenario described above, the retailer store will have to provide data subjects at least with clear notice about the following:

(i) the presence of RFID tags on products or their packaging and the presence of readers;

(ii) the consequences of such presence in terms of information gathering; in particular, data controllers should be very clear in informing individuals that the presence of such devices enables the tags to broadcast information without individuals engaging in any active action;

(iii) the purposes for which the information is intended to be used, including (a) the type of data with which RFID information will be associated and (b) whether the information will be made available to third parties and,

(iv) the identity of the controller.

(v) whether the voluntary or mandatory supply of the data is required or not for the processing of the information to take place.

(vi) What are the consequences of non-supply of the data for the data subject.

In addition, depending on the specific use/s of RFID, the data controller will also have to inform individuals about:

(v) how to discard, disable or remove tags from the products, thus preventing them from disclosing further information; and

(vi) how to exercise the right of access to information.

The principle of fair processing requires the information to be provided to data subject in a clear and comprehensible manner.

Finally, in providing the above information, the data subject should be in a position to understand easily the effects of the RFID application.

Data subject's right of access

The Data Protection Act gives data subjects the possibility of checking the accuracy of the data and ensuring the data are kept up to date. These rights fully apply to the collection of personal data through RFID technology. If we go back to the example of the supermarket which tags loyalty cards, providing for the right of access will entail disclosing *all* the information linked to a person, which may include the number of times the person entered the shop, the items bought, etc.

If RFID tags contain personal information as described above, individuals should be entitled to know the information contained in the tag and to make corrections using means easily accessible.

Security related obligations

The Data Protection Act imposes an obligation upon data controllers to implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or unauthorised disclosure.

Data security

Use of encryption on tags and applications: When RFID tags contain personal data, they must embed technical measures to prevent unauthorised disclosure of the data. Unless such measures are implemented, anyone with a reader could "wake up" a tag and obtain the information stored on it. Such measures are also necessary to ensure the integrity of the data stored in the tag, thus avoiding unauthorised changes.

The type of technical means will depend on the nature of the data. As further illustrated below, most of the time, these tags could require the *encryption* of the data and the authentication of the reader to prevent third parties provided with readers from reading the information. If we consider the scenario where RFID labels containing a patient's identity, the doctor is identified and procedure to be performed by the hospital staff, it is easy to understand the hospital's obligation to ensure that such information is not readable by third party readers which brings the subsequent need to use technical measures such as encryption to prevent it.

The most general and secure approach is the use of standard authentication protocols (e.g. ISO/IEC 9798). They are already widely used in networks or with smart cards. In these standardised protocols, cryptographic primitives are used. For symmetric authentication methods, which means that the keys for sender and

receiver are equal, MACs (message authentication codes) or symmetric encryption algorithms (e.g. DES, AES) are used. For asymmetric methods, where each party has a private and a public key, asymmetric encryption algorithms (e.g. RSA, ECC) or signature schemes are employed.

Some cryptographic authentication methods are already implemented in car immobilizers or access control systems, but they often use proprietary algorithms, because they are often easier and less expensive to implement than standard algorithms.

Nevertheless for enhanced security which may be needed to protect sensitive data, standard algorithms and protocols should be implemented. The advantage of such protocols and algorithms is that they are already widely used and therefore tested and challenged by many different parties. In that way, they are now broadly accepted as being secure.

LOCATION DATA

Background and purpose

There has been a spectacular increase in the use of location data in the last 20 years, driven by two main factors:-

The first is the explosion in the use of satellite location data, which today can be extremely precise and often very valuable, particularly when it comes to assisting individuals in distress. However, such systems are available only to those equipped with the appropriate terminals.

The second factor is the unprecedented spread of mobile telephony, where each user constantly carries about a device through which he or she can be potentially located.

Generally speaking, there are many ways of locating individuals, primarily using "traces" left by the use of new technologies: automatic ticket machines in the transport sector, GPS, bank cards or electronic purses, or, mobile telephones. At first, location data were regarded as purely technical data required for making or receiving a call from a mobile telephone and available only to electronic communications operators. The term "traffic" data is used in this connection. Such data merely result from the use of a given technology and are no different from other "traces" created every day.

Nevertheless, location data, insofar as they provide key information about an individual (in short, who is where), quickly came to be viewed as a potential source of revenue. Firms have developed a wide variety of services drawing on such data.

The first such services offered information to individuals on, for example, the nearest chemist or restaurant to their position. Next, services based on the one-off use of location data (providing information at a given moment in time) were supplemented by services based on continuous use of the data (navigational assistance).

This first stage has now given way to a second stage, with the development of services that are no longer based on locating people at their own request (users wishing to avail themselves of a service), but on their being located (at the request of a third party). Tracking and search services have developed whereby individuals can be located via their mobile phones even if they are not using them, but provided that they are switched on.

The key issue for the processing of location data has thus moved on from being a question of storage (essentially: on what conditions should location data be stored by electronic communications operators?) to being a question of use (how can we ensure that data are used for supplying value-added services in accordance with the principles applicable to the processing of personal data?).

Legal framework

Since location data always relate to an identified or identifiable natural person, they are considered personal data. The Data Protection Act defines traffic data as *"any data relating to a communication by means of a computer system and generated by the system that form part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service."*

General conditions governing the use of location data with a view to providing value-added services:-

Informing the data subjects:

The Data Protection Act requires that the subjects of location data to be processed be informed about:

- the collection of the data
- the purposes of processing
- the intended recipients of the data
- the name and address of the data controller
- the voluntary or mandatory supply of the data
- the identity of the controller and of his representative, if any
- the consequences of non-supply of the data for the data subject
- the type of processing to be conducted
- the right of access to and the right to rectify the data.

Obtaining consent:

Consent is defined as "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed".

Offering a service that requires the automatic location of an individual (e.g. the possibility of calling a specific number to obtain information on the weather conditions at one's location) is acceptable provided that users are given full information in advance about the processing of their location data. In this case, calling the relevant number would amount to consenting to being located.

A value-added service based on location data may be provided either directly by the electronic communications operator (the individual concerned contacts the operator, who then provides the service on the basis of the location data obtained from his system) or via a third party (the individual concerned contacts a third party, who then provides the service on the basis of the location data obtained from the operator).

In the second case, it is the service provider who must obtain the data subject's consent. Except where the location data is produced by the terminal equipment itself, this requires operators to systematically send location data for an identified individual (the person who contacted the third party in order to use the service) to a third party at the latter's request.

A high degree of protection in the processing of personal location data could be achieved if operators were to centralise requests to use a value-added service based on location data (customers calling a number managed by the operator) and transferring the requests to the third parties responsible for providing the service in such a way that the service provider cannot identify the customer (e.g. by using an alias). Under this arrangement, the service provider can deliver the service required (e.g. the name of the nearest restaurant) via the operator without being able to identify the person requesting the service. The end-user terminal could also provide a high degree of protection with its own built-in location capability. The location data can then be processed by an Identity Management System to deliver pseudonyms to multiple service providers.

Alternatively, and in view of constantly growing mobile bandwidth and storage capacities, the end-user device could for example download the full list of restaurants in a city and search locally in this list using not only the location data but the user's preferences as well (French cuisine, vegetarian menu, etc.). With these examples, the Commissioner underlines the need to consider Privacy Enhancing Technologies as efficient and complementary elements in providing a high and satisfactory degree of protection to users of geolocalisation services.

The Commissioner would draw operators' attention to the need to introduce effective measures to verify and authenticate requests for access to location data made by third parties offering a value-added service.

The Commissioner takes the view that providers of value-added services must take appropriate measures when obtaining consent to ensure that the person to whom the location data relate is the same as the person who has given consent. Where the processing of location data is ongoing (e.g. services such as Find-a-friend), the service provider must: confirm subscription to the service by sending a message to the user's terminal equipment after consent has been received, and - if necessary, request confirmation of the subscription.

This is to avoid cases of fraudulent subscription without the individual's knowledge (temporary removal of a person's terminal equipment in order to subscribe to the service).

Exercising the right to withdraw:

People who have given their consent for the processing of location data other than traffic data may withdraw consent and must have the possibility of temporarily refusing the processing of inaccurate data.

It is a precondition for the exercise of these rights that individuals are kept informed, not only when they subscribe to a service but also when they use it. Where a service requires ongoing processing of location data, the service provider should regularly remind the individual concerned that his or her terminal equipment has been, will be or can be located. This will allow that person to exercise the right to withdraw, should he or she wish to do so.

Data storage time:

Location data may be processed only for the period required.

This means that, once the service has been provided, the service provider may not in principle store individuals' location data, unless they are needed for billing and interconnection payment purposes.

Should service providers wish to keep a record of the locations of their service's users, they must first render the data anonymous.

Security measures and transmission to third parties:

The Commissioner would draw the attention of electronic communications operators and providers of value-added services based on the processing of location data to the need to introduce security measures designed to ensure the confidentiality and integrity of the location data processed.

Location data to be processed for providing a value-added service may not be transmitted to third parties other than those who provide the value-added service. Only persons acting under the authority of the third party providing the value-added service may process the data, to the extent and for the duration necessary for providing the service. Accesses by such persons to the location data should also be logged.

Conditions for implementing certain location services in the light of their purpose

The Data Protection Act stipulates that personal data may be used only "for specified and lawful purposes".

Location of minors

The development of location services designed for parents, allowing them, for example, to connect to a website in order to ascertain the location of their children, to whom they have given a mobile telephone. This type of service raises a number of problems, related in particular to the need for striking a balance between the different interests and rights at stake.

Media coverage of criminal cases involving children, the need to monitor children affected by certain illnesses or the emergence of an increasingly "nomadic" lifestyle may lead some parents to seek to be "reassured" by the possibility of locating their children at any time without having to call them direct. This new use of the mobile telephone for the benefit of parents, and at their expense, can be viewed as a sort of family "contract": greater independence of communication for the child in exchange for the possibility of being located by the parent.

In this respect, such services may meet an identified modern "need" and reflect a desire on the part of service providers to position themselves on a market which is likely to expand and which represents a new example of how the possibilities offered by location data are marketed.

However, this service could equally be looked at the other way around: from the point of view not of the parent, however understandable that point of view may be, but that of the child.

Articles 3 and 18 of the International Convention on the Rights of the Child state that the "best interests of the child shall be a primary consideration" in any decision concerning children. In the case at issue, one should also consider that Article 16 of the Convention provides that "no child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence".

Questions thus arise with respect to the use of this kind of service, which may possibly upset the normal relations of mutual trust between parents and their children and prevent children from gaining the necessary distance between themselves and their parents as they become more independent. Moreover, might not such a system, perversely, cause some parents to abandon their responsibility while maintaining the illusion of controlling — or at least monitoring — their children's activities? From a societal point of view, the development of this kind of service may also help to foster a surveillance system of individuals from a very young age to a semi-permanent form of monitoring which will no longer be considered intrusive?

Lastly, there is a risk that parents will confuse knowing where their child's mobile telephone is with knowing what the child is actually doing.

The Commissioner calls at least for vigilance in the use of this type of service and would point out that it must be implemented in accordance with the rules on the processing of location data and in accordance with specific local legislation regarding the age of the minors concerned.

Service providers must accordingly introduce appropriate procedures for identifying people who register as parents and for limiting access to the service to those people alone.

In addition, there is the question of the minor's consent to being the subject of a location request.

In this connection, the Commissioner notes that it may be nearly impossible to verify, when a location request is made, that the person using the telephone is the minor concerned and not someone else, perhaps an adult, to whom the subscriber to the service has entrusted the relevant telephone. She therefore recommends that the consent of the telephone user should be obtained, at least when the service is subscribed to. In order to prevent the fraudulent registration of telephones,

service providers should, for instance, send messages to the relevant telephone specifying that it has been the subject of a location request, so that the telephone user can in particular exercise the right to withdraw pursuant to the Data Protection Act.

Location of employees

Surveillance of workers must be carried out in the least intrusive way possible.

Data processing which allows an employer to collect data on the location of an employee, either directly (location of the employee him/herself) or indirectly (location of the vehicle used by the employee or of a product or asset in his/her charge) involves the use of personal data.

The Commissioner has observed the development of systems allowing companies to identify the geographic position of their staff at a given moment in time or continuously by locating objects in their possession (badge, mobile telephone, etc.) or use vehicles.

This information can be based on the processing of data from satellites (GPS), from an electronic communications network (mobile telephone, Wi-Fi network) or from any other device (such as an RFID tag located by a reader). It is increasingly being supplemented by data from various sensors which go beyond location data in the strict sense, e.g. data on the length of time for which a machine or vehicle is used, the number of kilometres covered or the speed at which a vehicle has travelled.

Such processing raises two issues: the demarcation line between work and private life and the degree of monitoring and permanent surveillance to which it is acceptable to subject an employee.

The Commissioner would like to recall, from a data protection point of view, that the lawfulness of such processing operations should not rely exclusively on the employee's consent, which must be "freely given" under the Data Protection Act. The issue of consent should be addressed in a broader perspective; in particular, the

the involvement of all the relevant stakeholders via collective agreements might be an appropriate way to regulate the gathering of consent statements in such circumstances.

Given the requirement that data be processed for specific purposes, the Commissioner takes the view that the processing of location data on employees must correspond to a specific need on the part of the company which is connected to its activity. Processing location data can be justified where it is done as part of monitoring the transport of people or goods or improving the distribution of resources for services in scattered locations (e.g. planning operations in real time), or where a security objective is being pursued in relation to the employee himself or to the goods or vehicles in his charge.

Conversely, the Commissioner considers data processing to be excessive where employees are free to organise their travel arrangements as they wish or where it is done for the sole purpose of monitoring an employee's work when this can be monitored by other means.

In these two cases, its purpose does not justify the use of undeniably intrusive processing given the type of data collected.

In any event, the purpose requirement means that an employer should not collect location data relating to an employee outside the latter's working hours. The Commissioner therefore recommends that equipment made available to employees, especially vehicles, which can also be used for private purposes be equipped with a system allowing employees to switch off the location function.

Location data relating to an employee must be kept for as long as is appropriate in view of the purpose advanced as justification for processing such data. Given the possible justifications for processing location data, processing will essentially be done in real time. In any event, the Commissioner recommends that the location data retention period be reasonable.

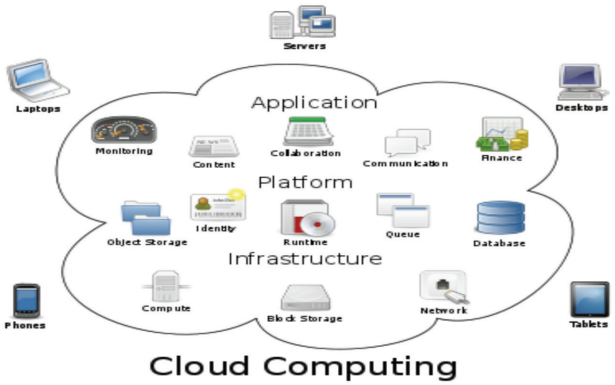
Where an employer wishes to process location data for long periods (e.g. to establish a historical record of journeys in order to optimise rounds), the Commissioner recommends that the data first be rendered anonymous.

Access to location data must be restricted to persons who, in the course of exercising their duties, may legitimately consult them in the light of their purpose. Employers must therefore take all necessary precautions in order

to keep such data secure and to prevent unauthorised access to them, in particular by introducing verification and identification measures.

Lastly, the Commissioner would highlight the obligation to inform the employees concerned and would draw data controllers' attention to the need to introduce location systems in such a way that staff are made aware of their existence.

CLOUD COMPUTING TECHNOLOGY



Cloud computing[3] is a technology developed for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or cloud provider interaction. Cloud computing technologies can be implemented in a wide variety of architectures, under different service and deployment models, and can coexist with other technologies and software design approaches. The security challenges cloud computing presents, however, are serious, especially for public clouds whose infrastructure and computational resources are owned by an outside party that sells those services[4] to the general public.

---

3 The common characteristics of cloud computing may be summarised as follows:- on-demand scalability of highly reliable pooled computing resources, secure access to metered services from nearly anywhere, and dislocation of data from inside to outside the organisation. While aspects of these characteristics have been realised to a certain extent, cloud computing remains a work in progress.

4 Three well-known and frequently-used service models are the following:

Software-as-a-Service - Software-as-a-Service (SaaS) is a model of software deployment whereby one or more applications and the computational resources to run them are provided for use on demand as a turnkey service. Its main purpose is to reduce the total cost of hardware and software development, maintenance, and operations. Security provisions are carried out mainly by the cloud provider. The cloud subscriber does not manage or control the underlying cloud infrastructure or individual applications, except for preference selections and limited administrative application settings.

Platform-as-a-Service - Platform-as-a-Service (PaaS) is a model of software deployment whereby the computing platform is provided as an on-demand service upon which applications can be developed and deployed. Its main purpose is to reduce the cost and complexity of buying, housing, and managing the underlying hardware and software components of the platform, including any needed program and database development tools. The development environment is typically special purpose, determined by the cloud provider and tailored to the design and architecture of its platform. The cloud subscriber has control over applications and application environment settings of the platform. Security provisions are split between the cloud provider and the cloud subscriber.

Infrastructure-as-a-Service - Infrastructure-as-a-Service (IaaS) is a model of software deployment whereby the basic computing infrastructure of servers, software, and network equipment is provided

Security and Privacy Issues and Precautions

Governance

- Extend organisational practices pertaining to the policies, procedures, and standards used for application development and service provisioning in the cloud, as well as the design, implementation, testing, and monitoring of deployed or engaged services.
- Put in place audit mechanisms and tools to ensure organisational practices are followed throughout the system lifecycle.

Compliance

- Understand the various types of laws and regulations that impose security and privacy obligations on the organisation and potentially impact cloud computing initiatives, particularly those involving data location, privacy and security controls, and electronic discovery requirements.
- Review and assess the cloud provider's offerings with respect to the organisational requirements to be met and ensure that the contract terms adequately meet the requirements.

Trust

- Incorporate mechanisms into the contract that allow visibility into the security and privacy controls and processes employed by the cloud provider, and their performance over time.
- Institute a risk management program that is flexible enough to adapt to the continuously evolving and shifting risk landscape.

Architecture

- Understand the underlying technologies the cloud provider uses to provision services, including the implications of the technical controls involved on the security and privacy of the system, with respect to the full lifecycle of the system and for all system components.
- Identity and Access Management
- Ensure that adequate safeguards are in place to secure authentication, authorisation, and other identity and access management functions.

Software Isolation

- Understand virtualisation and other software isolation techniques that the cloud provider employs, and assess the risks involved.

Data Protection

- Evaluate the suitability of the cloud provider's data management solutions for the organisational data concerned.

Availability

- Ensure that during an intermediate or prolonged disruption or a serious disaster, critical operations can be immediately resumed and that all operations can be eventually reinstituted in a timely and organised manner.

Incident Response

Understand and negotiate the contract[5]

as an on-demand service upon which a platform to develop and execute applications can be established. Its main purpose is to avoid purchasing, housing, and managing the basic hardware and software infrastructure components, and instead obtain those resources as virtualised objects controllable via a service interface.
The cloud subscriber generally has broad freedom to choose the operating system and development environment to be hosted. Security provisions beyond the basic infrastructure are carried out mainly by the cloud subscriber.

5 Service Agreements Specifications for public cloud services and service arrangements are generally called Service Level Agreements (SLAs). An SLA represents the understanding between the cloud subscriber and cloud provider about the expected level of service to be delivered and, in the event that the provider fails to deliver the service at the level specified, the compensation available to the cloud subscriber. An SLA, however, typically forms only a part of the terms of service stipulated in the overall service contract or service agreement. The terms of service cover other important details such as licensing of services, criteria for acceptable use, service suspension and termination, limitations on liability, privacy policy, and modifications to the terms of service.
Three main security and privacy issues in service contracts have been identified previously and are relevant to outsourcing public cloud computing services:-
Inadequate Policies and Practices - This can result in undetected intrusions or violations due to insufficient auditing and monitoring policies by the cloud provider; lack of sufficient data and configuration integrity due to a mismatch between the organisation's and the cloud provider's policies for separation of duty (i.e., clear assignment of roles and responsibilities) or redundancy (i.e., having sufficient checks and balances to ensure an operation is done consistently and correctly); and loss of privacy due to the cloud provider handling sensitive information less rigorously than the organisation's policy dictates.
Weak Confidentiality and Integrity Sureties - Insufficient security controls in the cloud provider's platform could affect negatively the confidentiality and privacy, or integrity of the system. For example, use of an insecure method of remote access could allow intruders

provisions and procedures for incident response required by the organisation.

Public cloud outsourcing

Below is a summary of the issues and the precautions that apply at the various stages of outsourcing.

Outsourcing Activities and Precautions Preliminary Activities

- Identify security, privacy, and other organisational requirements for cloud services to meet, as a criterion for selecting a cloud provider.
- Perform risk and privacy-impact assessments, analysing the security and privacy controls of a cloud
- provider's environment with respect to the control objectives of the organisation.
- Evaluate the cloud provider's ability and commitment to deliver cloud services over the target timeframe and meet the security and privacy levels stipulated.

Initiating and Coincident Activities

- Ensure that all contractual requirements are explicitly recorded in the SLA, including privacy and security provisions, and that they are endorsed by the cloud provider.
- Involve a legal advisor in the negotiation and review of the terms of service of the SLA.
- Continually assess the performance of the cloud provider and ensure all contract obligations are being met.

Concluding Activities

- Alert the cloud provider about any contractual requirements that must be observed upon termination.
- Revoke all physical and electronic access rights assigned to the cloud provider and recover physical tokens and badges in a timely manner.
- Ensure that resources made available to the cloud provider under the SLA are returned in a usable form, and confirm with evidence that information has been properly expunged.

Accountability for security and privacy in public clouds remains in principle with the organisation. Section 27 of the Data Protection Act explains the shared legal responsibilities between a data controller (the organisation) and a data processor (the cloud provider).

The data controller must ensure that any selected public cloud computing solution is configured, deployed, and managed to meet the security, privacy, and other requirements of the organisation.

Organisational data must be protected in a manner consistent with policies, whether in the organisation's computing center or the cloud. The organisation must ensure that security and privacy controls are implemented correctly and operate as intended.

---

to gain unauthorised access, modify, or destroy the organisation's information systems and resources; to deliberately introduce security vulnerabilities or malware into the system; or to launch attacks on other systems from the organisation's network, perhaps making it liable for damages.

Weak Availability Sureties - Insufficient safeguards in the cloud provider's platform could negatively affect the availability of the system. Besides the applications directly affected, a loss of system availability may cause a conflict for key resources that are required for critical organisational operations. For example, if disruptive processing operations are performed by the cloud provider (e.g., load rebalancing due to site failure or emergency maintenance) at the same time as peak organisational processing occurs, a denial of service condition could arise.

Principal-Agent Problem - The principal-agent problem occurs when the incentives of the agent (i.e., the cloud provider) are not aligned with the interests of the principal (i.e., the organisation)

Attenuation of Expertise - As new advancements and improvements are made to the cloud computing environment, the knowledge and expertise gained directly benefit the cloud provider, not the organisation. To remain accountable and mitigate the above-mentioned security and privacy issues, an organisation can carry out a number of activities at each of three distinct stages of the outsourcing lifecycle: when initiating, conducting, and concluding outsourced services. Non-negotiable SLAs generally limit the range of activities available to an organisation during the lifecycle, while negotiated SLAs, which provide greater range and flexibility, necessitate careful scrutiny and prioritisation of requirements that are incorporated into the terms of service in order to be cost effective. An organisation may be able to employ compensating controls to work around identified shortcomings in a public cloud service with a non-negotiable SLA. Another alternative is for the organisation to employ a cloud computing environment with a more suitable deployment model, such as a private cloud, which offers greater oversight and control over security and privacy.

CONCLUSION

Given the increasing use of PETs for a variety of purposes and applications, some of which with huge data protection implications, this document has been prepared on the basis of available information, considering the status of development of technology and particularly its current application in a variety of sectors. However, since the use of PETs is in continuous evolution: developments in this field occur constantly and as more experience is gained, the greater is the knowledge of the issues presented at stake.

REFERENCES

Picture: Cover
http://microsoft.office.com

Picture: PETs
http://eit.ictlabs.eu/action-lines/privacy-security-trust-in-information-society/

Picture: Fingerprint Technology
http://privacycouncil.org/fingerprinting-technology

Picture: Username/Password
http://www.mimos.my/research-development/rd-areas/information-security/

Picture: Internet Privacy Policy
http://www.infobarrel.com/Internet_Privacy_Policy_-_Protect_yourself_from_Reverse_Phone_Number_Lookup

Picture: Cookie Accept/Reject
http://etutorials.org/Linux+systems/moving+to+linux/Chapter+11.+Surfing+the+Net+Just+Browsing/Cool+Konqueror+Tricks/

Picture: Virtual Identity Manager
http://docs.oracle.com/cd/E19225-01/820-5822/byaap/index.html

Picture: TPM
http://forum.tabletpcreview.com/news-headlines/3757-do-i-need-trusted-platform-module-my-tablet-pc.html

Picture: RFID
http://workspacesolutions.com/blog/?tag=rfid

Picture: RFID_1
http://www.smartautomation.in/smart-tag-rfid-based-security/

Picture: Location Data
http://www.mobilemarketingwatch.com/mobile-location-data-gains-precision-with-twitter-places-api-and-simplegeo-updates-11962/

Picture: Cloud Computing
http://en.wikipedia.org/wiki/Cloud_computing

Designed and Printed by: The Government Printing Department, December 2012