Workshop on

"Cloud Computing, Social Networking and Online Behavioural Advertising"

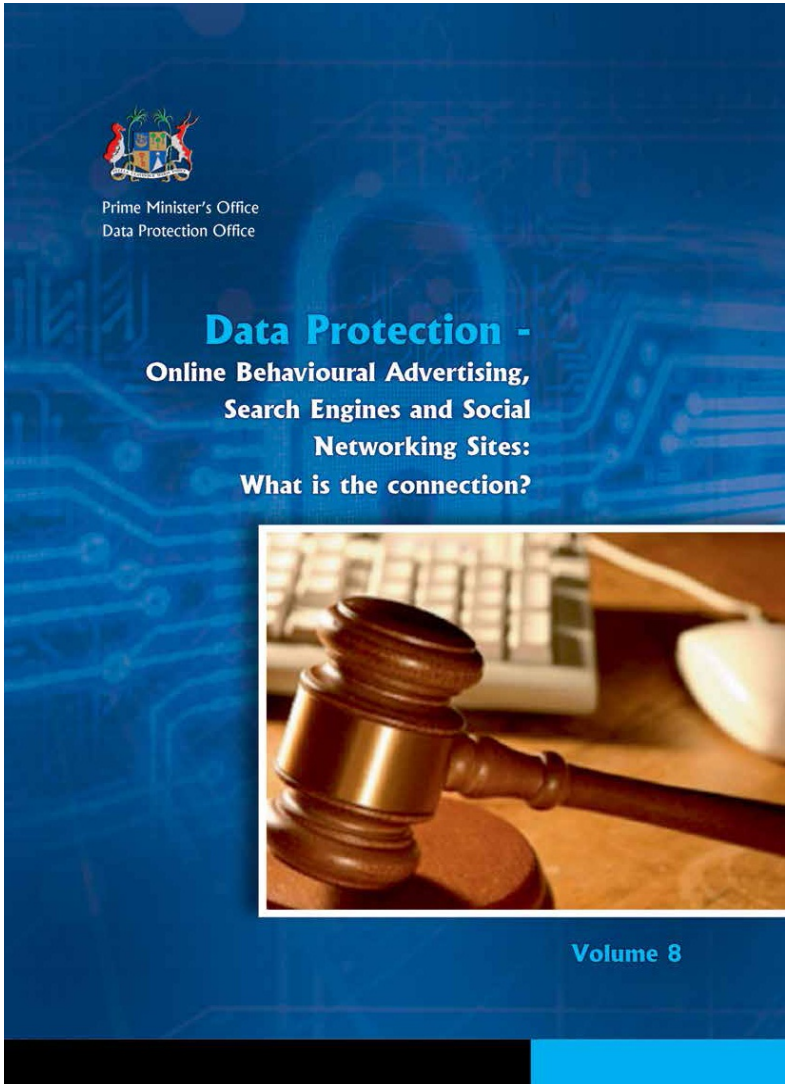
Data Protection Office

By : Mrs D. Madhub,
Data Protection Commissioner
Date : 17 Dec 2012
Venue : Le Maritim Hotel, Balaclava

Agenda

1. Cloud Computing
2. Practices
3. Social Networking Sites (SNS)
4. Obligations of SNS
5. Rights of Users/Third Party Access
6. User Mediated-Third Party Access
7. Online Behavioural Advertising
8. Applicability of DPA, Obligations and Rights

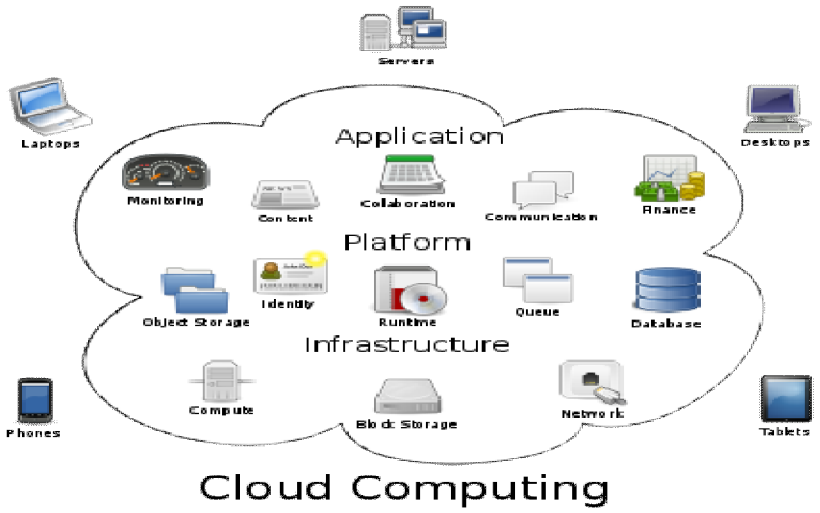
Guidelines issued by Data Protection Commissioner



1.What is Cloud Computing ?

Cloud computing 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.

The data protection challenges cloud computing presents, however, are serious, especially for public clouds whose infrastructure and computational resources are owned by an outside party which sells those services to the general public.



1.Cloud Computing

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.

1.Cloud Computing(cont'd)

❖**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 a special purpose, determined by t*he *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.**

1.Cloud Computing (cont'd)

- **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 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.**

2.Cloud Computing (Practices)

Good practices:-

Governance

- Extend internal and external organisational practices pertaining to the policies, procedures, and standards used for application development and service provisioning to the cloud.
- Put in place audit mechanisms and tools to ensure the 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

2.Cloud Computing (Practices)

- 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.

2.Cloud Computing (Practices)

- 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.

2.Cloud Computing (Practices)

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.

2.Cloud Computing (Practices)

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 provisions and procedures for incident response required by the organisation.

2.Cloud Computing (Practices)

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:-

- 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 above privacy levels.

2.Cloud Computing (cont'd)

- **Concluding Precautions:-**
- 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 evidence that information has been properly expunged.
- Note that accountability for security and privacy in public clouds remains with the organisation.

2.Cloud Computing (cont'd)

- 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.

3.Social Networking Sites (SNS)

3. What are Social Networking Sites?

- ***SNS can broadly be defined as online communication platforms which enable individuals to join or create networks of like-minded users.***
- SNS generate much of their revenue through advertising which is served alongside the web pages setup and accessed by users. Users who post large amounts of information about their interests on their profiles offer a refined market to advertisers wishing to serve targeted advertisements based on that information.

3.What is Social Networking Sites?

SNS share certain characteristics:

- Users are invited to provide personal data for the purpose of generating a description of themselves or ‘profile’.
- SNS also provide tools which allow users to post their own material (user-generated content such as a photograph or a diary entry, music or video clip or links to other sites).
- ‘Social networking’ is enabled using tools which provide a list of contacts for each user, and with which users can interact.

3.Social Networking Sites (cont'd)

❖It is therefore important that SNS as data controllers operate in a way which respects the rights and freedoms of users (data subjects) who have a legitimate expectation that the personal data they disclose will be processed in accordance with data protection principles.

❖Data Controllers must take the appropriate technical and organisational measures, both at the time of the design of the processing system and at the time of the processing itself to maintain security and prevent unauthorised processing, taking into account the risks represented by the processing and the nature of the data.

3.Social Networking Sites (cont'd)

- The personal information a user posts online, combined with data outlining the users' actions and interactions with other people, can create a rich profile of a person's interests and activities. Personal data published on social network sites can be used by third parties for a wide variety of purposes, Including commercial purposes, and may pose major risks such as identity theft, financial loss, loss of business or employment opportunities and physical harm.

3.Social Networking Sites (cont'd)

- SNS providers should inform users of their identity from the outset and outline all the different purposes for which they process personal data in accordance with section 22 of the Data Protection Act.

The dissemination and use of information available on SNS for other secondary, unintended purposes is of key concern to the office. Robust security and privacy-friendly default settings are advocated throughout the guide as the ideal starting point with regard to all services on offer.

3.Social Networking Sites (cont'd)

- SNS should also provide comprehensive and clear information about the purposes and different ways in which they intend to process personal data. SNS should offer privacy-friendly default settings.
- SNS should provide adequate warnings to users about privacy risks when they upload data onto the SNS.
- Users should be advised by SNS that pictures or information about other individuals should only be uploaded with the individual's consent.

4.Obligations of SNS

- At a minimum, the homepage of SNS should contain a link to a complaint facility, covering data protection issues, for both members and non-members.
- A large proportion of SNS services are utilised by children/minors. There is thus a need for taking into account the best interest of the child as also set out in the UN Convention on the Rights of the Child. Based on the considerations made so far, a multi-pronged strategy would be appropriate to address the protection of children's data in the SNS context.

4.Obligations of SNS

Such a strategy might be based on:

- awareness raising initiatives, which are fundamental to ensure the active involvement of children (via schools, the inclusion of DP-basics in educational curricula, the creation of ad-hoc educational tools, the collaboration of national competent bodies);
- fair and lawful processing with regard to minors such as not asking for sensitive data in the subscription forms, no direct marketing aimed specifically at minors, the prior consent of parents before subscribing, and suitable degrees of logical separation between the communities of children and adults;

4.Obligations of SNS

- implementation of Privacy Enhancing Technologies (PETs) - e.g. privacy-friendly settings by default, pop-up warning boxes at appropriate steps, age verification software;

- self-regulation by providers, to encourage the adoption of codes of practice, under the guidance of the Data Protection Commissioner, that should be equipped with effective enforcement measures, also disciplinary in nature.

5.Rights of Users

- Many SNS allow users to contribute data about other people, such as adding a name to a picture, rating a person, listing the “people I have met/want to meet” at events. This tagging may also identify non members. However, the processing of such data about non-members by the SNS may only be performed if the criteria laid down in the Data Protection Act are fulfilled. In addition, the creation of pre-built profiles of non-members through the aggregation of data that is independently contributed by SNS users, including relationship data inferred from uploaded address books, lacks a legal basis.

5.Third Party Access

SNS-mediated access:-

- In addition to the core SNS service, most SNS offer users additional applications provided by third party developers who also process personal data as data controllers or processors.

- SNS should have the means to ensure that third party applications comply with the Data Protection Act. This implies, in particular, that they provide clear and specific information to users about the processing of their personal data and that they only have access to necessary personal data.

5.Third Party Access

- Therefore, layered access should be offered to third party developers by the SNS so they can opt for a mode of access that is intrinsically more limited.
- SNS should ensure furthermore that users may easily report concerns about applications.
- SNS sometimes allow users to access and update their data with other applications. For example, users might be able to read and post messages to the network from their mobile phones;
- synchronize the contact data of their friends in the SNS with their address books on a desktop

6.User Mediated-Third Party Access

computer; update their status or location in the SNS automatically by using another website.

- This software can be written in the form of an “Application Programming Interface” (“API”) which refers to access whereby users need to provide their login credentials to the software, so that it can act on their behalf.
- When accessing personal data via third party’s API on behalf of a user, third party services should:
  - process and store data no longer than necessary to perform a specific task;
  - perform no operations on imported user contacts' data other than
  - personal usage by the contributing user.

6.User Mediated-Third Party Access(cont'd)

- Some SNS allow their users to send invitations to third parties. The practice by some SNS to send invitations indiscriminately to the entire address book of a user is not allowed. Some SNS also retain identification data of users who were banned from the service, to ensure that they cannot register again.
- In that case, these users must be informed that such processing is taking place. In addition, the only information that may be retained is identification information, and not the reasons why these persons were banned.

6.User Mediated-Third Party Access(cont'd)

- Personal data communicated by a user when he registers to a SNS should be deleted as soon as either the user or the SNS provider decides to delete the account. Similarly, information deleted by a user when updating his account should not be retained. SNS should notify users before taking these steps with the means they have at their disposal to inform users about these retention periods.
- For security and legal reasons, in specific cases, it could be justifiable to store updated or deleted data and accounts for a defined period of time in order to help prevent malicious operations resulting from identity theft and other offences or crimes.

6.User Mediated-Third Party Access(cont'd)

- When a user does not use the service for a defined period of time, the profile should be set to inactive, i.e. no longer visible to other users or the outside world, and after another period of time the data in the abandoned account should be deleted.
- SNS should notify users before taking these steps with whatever means they have at their disposal.

7.Online Behavioural Advertising (OBA)

1. A person visits a web page about Rome

2. Some time later they visit a football site and an offer for cheap hotels in Rome appears

7.What is Online Behavioural Advertising?

What is Online Behavioural Advertising ?

- Online Behavioural Advertising means the collection of data from a particular computer or device regarding web viewing behaviours over time and across multiple web domains for the purpose of using such data to predict web user preferences or interests to deliver online advertising to that particular computer or device based on the preferences or interests inferred from such web viewing behaviours. It does not include the activities of Web Site Operators, Ad Delivery or Ad Reporting, or contextual advertising (e.g. advertising on the content of the web page being visited, a consumer's current visit to a web page, or a search query).

7.Online Behavioural Advertising (cont'd)

- Online advertising is a vital source of income for a wide range of online services and is an important catalyst in the growth and expansion of the internet economy. However, the particular practice of behavioural advertising also raises important data protection and privacy related concerns.

- Basic internet technology allows advertising network providers to track data subjects across different websites and over time. Such profiles can be used to provide data subjects with tailored advertising.

.

7.Online Behavioural Advertising (cont'd)

Behavioural advertising involves the following actors:

- **Advertising network providers (also referred to as "ad network providers"), the most important distributors of behavioural advertising since they connect publishers with advertisers;**

- **Advertisers who want to promote a product or service to a specific audience; and**

- **Publishers who are the website owners looking for revenues by selling space to display ads on their website(s).**

8.Applicability of DPA , Obligations and Rights

- Providing highly visible information is a precondition for consent to be valid. Mentioning the practice of behavioural advertising in general terms and conditions and/or privacy policies can never suffice.
- Notices provided in general terms and conditions and/or privacy policies, often drafted in rather obscure ways fall short of the requirements of the Data Protection Act.
- In this regard and taking into account the average low level of knowledge about the practice of behavioural advertising, efforts should be applied to change this situation. In practical terms, data controllers should ensure that individuals are told, at a minimum, who (i.e. which entity) is responsible for serving the cookie and collecting the related information.

8.Applicability of DPA , Obligations and Rights

In addition, they should be informed in simple ways:

- that the cookie will be used to create profiles;
- what type of information is required to be collected to build such profiles;
- that the profiles will be used to deliver targeted advertising, and,
- that the cookie will enable the user's identification across multiple web sites.

8.Applicability of DPA , Obligations and Rights (Cont'd)

- Behavioural advertising involves the processing of unique identifiers that are achieved through the use of cookies, or any kind of device fingerprinting. The use of such unique identifiers allows for the tracking of users of a specific computer even when IP addresses are deleted or anonymised. In other words, such unique identifiers enable data subjects to be "singled out" for the purpose of tracking user behaviour while browsing on different websites and thus qualify as personal data.

8.Applicability of DPA , Obligations and Rights

- Specific software applications (browser plug-ins or extensions) could be developed by ad networks and downloaded and installed by users to enable changing the status of browser settings with regard to advertising-related cookies by means of application programming interfaces (API) or other tools made available by browser manufacturers. Users should receive the relevant information on data processing as a preliminary step to installing the specific “advertising” plug-in.

The Data Protection Act 2004 is applicable when behavioural advertising is based on the use of identifiers that enable the creation of very detailed user profiles which, in most cases, are personal data.

8.Applicability of DPA , Obligations and Rights (Cont'd)

Such a privacy solution is 'Do Not Track', a consent mechanism based on browser settings. However, such a mechanism should truly enable users to express their consent on a case by case basis, without being tracked by default.

- Network providers/ publishers should provide the information directly on the screen, interactively, if needed, through layered notices and it should be easily accessible.
- Icons placed on the publishers' website, around advertising, with links to additional information, are good examples. Network providers/publishers should be creative in this area.

8.Applicability of DPA , Obligations and Rights

- Browsers must either alone or in combination with other means effectively convey clear, comprehensive and fully visible information about the processing.
- Ad network providers should encourage and work with browser manufacturers/ developers to implement privacy by design in browsers.
- Cookie-based opt-out mechanisms in general are not sufficient to constitute an adequate mechanism to obtain informed and express user consent. Though, in most cases, express user's consent may also be implied if they do not opt out, this does not stand to mean that the decision not to opt out is an informed one.

8.Applicability of DPA , Obligations and Rights

- In practice, very few people exercise the opt-out option, not because they have made an informed decision to accept behavioural advertising, but rather because they are not aware that the processing of their personal data is taking place, and/or do not know how to exercise the opt out option.
- Although the opt-out cookie prevents the further reception of personalised advertising, it does not stop the advertising network from accessing and storing information in the user's terminal. On the contrary, it has been demonstrated that an ongoing technical exchange of information between the user’s terminal equipment and the advertising network is still in place after the installation of the opt-out cookie.

8.Applicability of DPA , Obligations and Rights

- The user is not informed on whether or not the tracking cookie remains stored in his/her computer and for what purpose/s. The installation of the opt-out cookie does not offer the possibility to manage and delete previously installed tracking cookies, whereas at the same time it creates the mistaken presumption that opting out disables the tracking of internet behaviour.

It is to be noted that express consent as provided in the Data Protection Act does not automatically relate to mandatory written consent but may also be implied and non- written.

8.Applicability of DPA , Obligations and Rights (Cont'd)

- Ad network providers should create prior opt-in mechanisms. Mechanisms to deliver informed, valid consent should require an affirmative action by the data subject indicating his/her willingness to receive cookies and the subsequent monitoring of his/her surfing behaviour for the purposes of sending him/her tailored advertising.

- A users' acceptance to receive a cookie could also entail his/her acceptance for the subsequent readings of the cookie, and hence for the monitoring of his/ her internet browsing. It would not be necessary to request consent for each reading of the cookie.

8.Applicability of DPA , Obligations and Rights

- However, to ensure that data subjects remain aware of the monitoring over time, ad network providers should:

  i) limit in time the scope of the express consent;

  ii) offer the possibility to easily revoke their consent to being monitored for the purposes of serving behavioural advertising and;

  iii) create a symbol or other tools which should be visible in all the web sites where the monitoring takes place (the website partners of the ad network provider). This symbol would not only remind individuals of the monitoring but also help them to control whether they want to continue being monitored or wish to revoke their consent.

8.Applicability of DPA , Obligations and Rights (Cont'd)

Pop up screens are not the only way to obtain consent. There are many other ways to obtain consent. Some of these examples are:

-A static information banner on top of a website requesting the user's consent to set some cookies, with a hyperlink to a privacy statement with a more detailed explanation about the different controllers and the purposes of the processing.

8.Applicability of DPA , Obligations and Rights (Cont'd)

- As an example, the following cookies would be exempted from informed consent:

  - ***A secure login session cookie.*** This type of cookie is designed to identify the user once he/she has logged-in to an information society service and is necessary to recognise him/her, maintaining the consistency of the communication with the server over the communication network.

  - ***A shopping basket cookie.*** On a shopping website, this type of cookie is typically used to store the reference of items the user has selected by clicking on a button (e.g. "add to my shopping cart"). This cookie is thus necessary to provide an information society service explicitly requested by the user.

8.Applicability of DPA , Obligations and Rights

Security cookies

- Cookies which provide security that are essential to comply

with the security requirements of the Data Protection Act for an information society service explicitly requested by the user. For example, a cookie may be used to store a unique identifier to allow the information society service to provide additional assurance . Attempted logins from unseen devices could prompt for additional security questions.

8.Applicability of DPA , Obligations and Rights (Cont'd)

- A splash screen on entering the website explaining what cookies will be set, by what parties, if the user consents.

  - A default setting prohibiting the transfer of data to external parties, requiring a user click to indicate consent for tracking purposes.

  - A default setting in browsers that would prevent the collection of behavioural data (Do not collect).

8.Applicability of DPA , Obligations and Rights

- Network providers should ensure compliance with the purpose limitation principle and security obligations. In addition, the ad network providers should enable individuals to exercise their rights of access and rectification and erasure. For instance, some ad network providers offer data subjects the possibility to access and modify the interest categories in which they have been classified. Ad network providers should implement retention policies which ensure that information collected .Each time that a cookie is read is automatically deleted after a justified period .

8.Applicability of DPA , Obligations and Rights (Cont'd)

Ad network providers are bound by the obligations of data controllers insofar as they place cookies and/or retrieve information from cookies already stored in the data subjects' terminal equipment and determine the purposes and the essential means of the processing of data. Ad network providers have complete control over the purposes and means of the processing.

8.Applicability of DPA , Obligations and Rights

- They 'rent' space from publishers' web sites to place adverts and, in most cases, collect the IP Address and possible other data that the browser may reveal. Further, the ad network providers use the information gathered on Internet users' surfing behaviour to build profiles and to select and deliver the ads to be displayed on the basis of this profile. In this scenario, they clearly act as data controllers, falling within the definition provided in the Data Protection Act.

8.Applicability of DPA , Obligations and Rights (Cont'd)

- Publishers, amongst others, rent out space on their websites for ad networks to place adverts. They set up their web sites in a way that visitors' browsers are automatically redirected to the webpage of the ad network provider (which will then send a cookie and serve tailored advertising). This raises the question about their responsibility vis-à-vis the data processing.

- Whether a publisher can be deemed to be a joint controller or a data processor with the Ad network provider will depend on the conditions of collaboration between the publisher and the ad network provider.

8.Applicability of DPA , Obligations and Rights (Cont'd)

- In this regard, it is necessary to interpret the legal framework in a flexible way by applying only those provisions that are pertinent. If publishers do not hold personal information, obviously, it would not make legal sense to apply some of the obligations of the Data Protection Act.

Publishers will be joint controllers if they collect and transmit personal data regarding their visitors such as name, address, age, location, etc to the ad network provider. To the extent that publishers act as data controllers or processors, they are bound by the obligations arising under the DPA regarding the part of the data processing under their control.

8.Applicability of DPA , Obligations and Rights

- In sum, publishers should be aware that by entering into contracts with ad networks with the consequence that personal data of their visitors are available to ad network providers, they take some responsibility towards their visitors. The breadth of their responsibility, including the extent to which they become data controllers or processors should be analysed on a case by case Accordingly, the service agreements between publishers and ad network providers should set up the roles and responsibilities of both parties in the light of their collaboration, as described in the agreement.

8.Applicability of DPA , Obligations and Rights (Cont'd)

- Publishers may also have certain data controller and processor related responsibilities regarding the processing that takes place in the first phase of the processing, i.e., when they set up their web sites, they trigger the transfer of the IP address as data controllers to ad network providers (which enable the further processing), such responsibility entails some data protection obligations. Thus, when publishers transfer directly identifiable personal data to ad network providers themselves, they will be deemed joint controllers.

8.Applicability of DPA , Obligations and Rights (Cont'd)

For browser settings to be able to deliver informed consent, it should not be possible to "bypass" the choice made by the user in setting the browser. Browser settings play in ensuring that data subjects effectively give their consent to the storage of cookies and the processing of their information, it seems of paramount importance for browsers to be provided with default privacy-protective settings, in other words, to be provided with the setting of 'non-acceptance and non-transmission of third party cookies'. To make it more effective, the browsers should require users to go through a privacy wizard when they first install or update the browser and provide for an easy way of exercising choice during use.

8.Applicability of DPA , Obligations and Rights (Cont'd)

- Even if, technically the data transfer of the IP address is carried out by the browser of the individual who visits the publisher's web site, it is not the individual who triggers the transfer.
- When a data subject clicks on an ad and visits the advertisers' website, the advertiser can track which campaign resulted in the click-through. If the advertiser captures the targeting information and combines it with the data subject's onsite surfing behaviour or registration data, then the advertiser is an independent data controller for this part of the data processing.

8.Children's Consent

- The problems related to obtaining informed consent are further emphasised as far as children are concerned. In addition to the requirements described above (and below) for consent to be valid, in some cases children's consent must be provided by their parents or other legal representatives. This means that ad network providers would need to inform parents about the collection and the use of children's information and obtain their consent before collecting and further using their information for the purposes of engaging in behavioural targeting of children.

8.Children's Consent

Taking into account the vulnerability of children, the office is of the view that ad network providers should not offer interest categories intended to serve behavioural advertising or influence children.

- Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, data concerning health or sex life or data related to criminal proceedings are considered sensitive. There are serious risks to the infringement of the personal data of individuals if this type of information is used for the purposes of serving behavioural advertising.

8.Obligations with regard to sensitive data

- Any possible targeting of data subjects based on sensitive information opens the possibility of abuse. Furthermore, given the sensitivity of such information and the possible awkward situations which may arise if individuals receive advertising that reveals, for example, sexual preferences or political activity, offering interest categories that would reveal sensitive data should be discouraged.
- Publishers may also be liable under general principles of civil law as well as consumer protection laws related to business-to-consumer commercial practices to inform individuals insofar as the data processing and monitoring takes place as a result of their action to re-direct them to the ad network provider.

8.Obligations with regard to sensitive data

- However, if nevertheless, ad network providers offer and use interest categories that reveal sensitive information, they must comply with data protection principles. For example, if an ad network provider processes individual behaviour in order to 'place him/her' in an interest category indicating a particular sexual preference, they would be processing sensitive data under section 25 of the Data Protection Act.

8.Obligations with regard to sensitive data (cont'd)

- This section prohibits the processing of sensitive data except in certain specific circumstances. If ad network providers want to use information gathered for behavioural advertisement for secondary, incompatible purposes, for example across services, they need additional legal grounds to do so. For example, they will need to inform data subjects and, in most cases, obtain their express consent. Compliance with the retention principle requires limiting the storage of information. Accordingly, companies must specify and respect timeframes under which data will be retained.

8.Obligations with regard to sensitive data (cont'd)

Pursuant to the above, information about users' behaviour has to be eliminated if it is no longer needed for the development of a profile. Indefinite or overly long retention periods contradict the Data Protection Act. Retention periods of major ad network providers may vary, with some companies using an indefinite period and others limiting the retention periods to a determined period.

8.Obligations with regard to sensitive data (cont'd)

- Accordingly, ad network providers should implement policies to ensure that information collected each time a cookie is read, is immediately deleted or anonymised once the necessity for retaining it has expired.
- Each data controller needs to be able to justify the necessity for a given retention period. Ad network providers should provide reasons that justify the conservation period that they consider necessary in the light of the purposes sought by the data processing.

8.Obligations with regard to sensitive data (cont'd)

- If/when an individual asks for a deletion of his/her profile or if he/she exercises his/her right to withdraw the consent, these actions require the ad network provider to erase or delete promptly the data subject's information in so far as the ad network provider ceases to have the necessary legal grounds allowing the processing.

Thanking You For Your Attention

Contact Us

DATA PROTECTION OFFICE

4th Floor, Emmanuel Anquetil Building,

Port Louis

Website: http://dataprotection.gov.mu

Telephone: 201 3962

Helpdesk: 203 90 76

Email: pmo-dpo@mail.gov.mu