• Do not store or request users to upload file containing personal data in webserver without proper protection such as access control and/or encryption. Use of passwords and where encryption may be a legal requirement. All personnel involved in the handling of personal data should be trained and gain understanding of the requirements of the Ordinance and the compliance procedures in place.

• Promote a privacy-aware culture in the workplace.

Every employee should be made aware of the importance of respecting the data privacy rights of individuals, both as a moral obligation and as a legal requirement. All personnel involved in the handling of personal data should be trained in understanding the requirements of the Ordinance and the compliance procedures in place.

• Set an action plan for data breach handling.

Data leakage on the Internet can spread quickly and widely, and immediate action to contain the leakage may cause irreversible damage to the reputation of an organisation. A transparent breach handling system should therefore be in place to avoid a clear action plan to be followed to contain any breaches, and to mitigate the damage caused to the data subjects concerned.

The engagement of data processors

DPP4(2) provides that if a data user engages a data processor, whether within or outside Hong Kong, to process personal data on the data user’s behalf, the data processor, whether within or outside Hong Kong, to process personal data on the data user’s behalf, the data

For details on how to prepare a DPP, organisations may refer to “Guidance on Preparing Personal Information Collection Statement and Privacy Policy Statement”.  

DPP6 – Access to Personal Data

Under DPP6, individuals have the right to request access to, and correction of, their personal data held by an organisation. There is no difference in treatment, no matter whether the personal data is collected or held online or offline by an organisation. The PCPD website has further information on how to handle data requests and data correction requests.

DPPS – Transparency of Policies and Practices

Openness of the organisation’s personal data privacy policy

DPP5 stipulates openness by organisations about their policies and practices in relation to personal data. An organisation with a website should make its privacy policy statement (“DPP”) either accessible or downloadable by web users. A DPP should define:

• Make the privacy policy statement easy to access.

One possible method of ensuring easy access is to set up the DPP as a linked page accessible from the organisation’s privacy policy statement (“DPP”), for example, by linking the DPP to the personal information collection statement. The link should be clearly labelled, for example, with a heading such as “Privacy Policy” or in the form of a button or icon carrying with similar meaning.

• State the privacy policy clearly.

The DPP should inform users of the kinds of personal data held by the organisation and the main purposes for which the personal data is used or to be used. It should also contain information about other matters relating to the privacy of personal data, such as the use, if any, of cookies by the organisation to track its visitors, the organisation’s policy on direct marketing, and its security and retention policies in relation to personal data.

Organisations should refer to the “New Guidance on Direct Marketing” for more details.

Data user should note that, Part VI A of the Ordinance concerning the requirements on direct marketing should be adequate data to be obtained through the Internet or form data subjects or, and whether the direct marketing activities are conducted in or via conventional ways.

• Should observe and comply with the relevant provisions under the Unofficial Electronic Messages Ordinance (Cap. 591), which is administered by the Office of the Communications Authority, in carrying out direct marketing activities by electronic messages.

Guidance for Users on the Collection and Use of Personal Data through the Internet

Introduction

Operating online businesses or services, whether by commercial enterprises, non-government organisations or public bodies, is now commonplace. In many cases, collecting such transactions involves the collection of personal data.

The personal data (privacy) (the Ordinance) provides for six data protection principles ("DPPs") which set out fairness information practices on how personal data should be handled by data users. A data user is defined as "a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data". The personal data protection law is administered by the Office of the Privacy Commissioner for Personal Data (PCPD).

The PCPD website has further information on how to handle data requests and data correction requests.

• Consider installing a data loss prevention system.

• Consider the use of privacy-enhancing technologies whenever possible to protect personal data.

Privacy-enhancing technologies are measures that help to minimise the risk of personal data exposure, such as encryption or hashing to mask data content, refusing access to, or closing access to, personal data. A website is described as "a website that is not linked to any company's main website". A web server is described as "a server that is located on the Internet and where a website and its related content can be viewed and/or browsed".

• Make the privacy policy statement easy to access.

One possible method of ensuring easy access is to set up the DPP as a linked page accessible from the organisation’s privacy policy statement (“DPP”), for example, by linking the DPP to the personal information collection statement. The link should be clearly labelled, for example, with a heading such as “Privacy Policy” or in the form of a button or icon carrying with similar meaning.

For details on how to prepare a DPP, organisations may refer to “Guidance on Preparing Personal Information Collection Statement and Privacy Policy Statement”.

DPP6 – Access to Personal Data

Under DPP6, individuals have the right to request access to, and correction of, their personal data held by an organisation. There is no difference in treatment, no matter whether the personal data is collected or held online or offline by an organisation. The PCPD website has further information on how to handle data requests and data correction requests.

DPPS – Transparency of Policies and Practices

Openness of the organisation’s personal data privacy policy

DPP5 stipulates openness by organisations about their policies and practices in relation to personal data. An organisation with a website should make its privacy policy statement (“DPP”) either accessible or downloadable by web users.

For details on how to prepare a DPP, organisations may refer to “Guidance on Preparing Personal Information Collection Statement and Privacy Policy Statement”.

DPP6 – Access to Personal Data

Under DPP6, individuals have the right to request access to, and correction of, their personal data held by an organisation. There is no difference in treatment, no matter whether the personal data is collected or held online or offline by an organisation. The PCPD website has further information on how to handle data requests and data correction requests.

Direct Marketing Activities

Organisations engaged in direct marketing activities using personal data must comply with Part VI A of the Ordinance regarding direct marketing activities.

Organisations should refer to the “New Guidance on Direct Marketing” for more details.

Data user should note that, Part VI A of the Ordinance concerning the requirements on direct marketing should be adequate data to be obtained through the Internet or form data subjects or, and whether the direct marketing activities are conducted in or via conventional ways.

Organisations should observe and comply with the relevant provisions under the Unofficial Electronic Messages Ordinance (Cap. 591), which is administered by the Office of the Communications Authority, in carrying out direct marketing activities by electronic messages.

Guidance for Users on the Collection and Use of Personal Data through the Internet

Introduction

Operating online businesses or services, whether by commercial enterprises, non-government organisations or public bodies, is now commonplace. In many cases, collecting such transactions involves the collection of personal data.

The personal data (privacy) (the Ordinance) provides for six data protection principles ("DPPs") which set out fairness information practices on how personal data should be handled by data users. A data user is defined as "a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data". The personal data protection law is administered by the Office of the Privacy Commissioner for Personal Data (PCPD).

The PCPD website has further information on how to handle data requests and data correction requests.

• Consider installing a data loss prevention system.

• Consider the use of privacy-enhancing technologies whenever possible to protect personal data.

Privacy-enhancing technologies are measures that help to minimise the risk of personal data exposure, such as encryption or hashing to mask data content, refusing access to, or closing access to, personal data. A website is described as "a website that is not linked to any company's main website". A web server is described as "a server that is located on the Internet and where a website and its related content can be viewed and/or browsed".

• Make the privacy policy statement easy to access.

One possible method of ensuring easy access is to set up the DPP as a linked page accessible from the organisation’s privacy policy statement (“DPP”), for example, by linking the DPP to the personal information collection statement. The link should be clearly labelled, for example, with a heading such as “Privacy Policy” or in the form of a button or icon carrying with similar meaning.

For details on how to prepare a DPP, organisations may refer to “Guidance on Preparing Personal Information Collection Statement and Privacy Policy Statement”.

DPP6 – Access to Personal Data

Under DPP6, individuals have the right to request access to, and correction of, their personal data held by an organisation. There is no difference in treatment, no matter whether the personal data is collected or held online or offline by an organisation. The PCPD website has further information on how to handle data requests and data correction requests.

DPPS – Transparency of Policies and Practices

Openness of the organisation’s personal data privacy policy

DPP5 stipulates openness by organisations about their policies and practices in relation to personal data. An organisation with a website should make its privacy policy statement (“DPP”) either accessible or downloadable by web users.

For details on how to prepare a DPP, organisations may refer to “Guidance on Preparing Personal Information Collection Statement and Privacy Policy Statement”.

DPP6 – Access to Personal Data

Under DPP6, individuals have the right to request access to, and correction of, their personal data held by an organisation. There is no difference in treatment, no matter whether the personal data is collected or held online or offline by an organisation. The PCPD website has further information on how to handle data requests and data correction requests.

Direct Marketing Activities

Organisations engaged in direct marketing activities using personal data must comply with Part VI A of the Ordinance regarding direct marketing activities.

Organisations should refer to the “New Guidance on Direct Marketing” for more details.

Data user should note that, Part VI A of the Ordinance concerning the requirements on direct marketing should be adequate data to be obtained through the Internet or form data subjects or, and whether the direct marketing activities are conducted in or via conventional ways.

Organisations should observe and comply with the relevant provisions under the Unofficial Electronic Messages Ordinance (Cap. 591), which is administered by the Office of the Communications Authority, in carrying out direct marketing activities by electronic messages.
Collecting personal data through the Internet

DPP1(3) sets out the information that a data user has to provide to an individual on or before collecting personal data, either in written forms or on their websites to collect personal data from individuals or ask them to submit their personal data via email or other electronic means. It should be made easy to make all reasonably practicable steps to ensure that individuals providing their personal data are supplied with the information required by DPP1(3).

Provide an online Personal Information Collection Statement. A practical way to comply with DPP1(3) is to provide the individual with an online Personal Information Collection Statement (“PICS”). A PICS should be displayed in a clear and conspicuous manner (e.g., accessible on the same web page or through a link on the page). It should be easy to make and understand, and its content must be consistent with any printed version distributed offline. Generally, a PICS should include the following information:

• Whether it is obligatory or voluntary for the individual to supply the data, and where it is obligatory, the consequences for failure to supply the data;
• The purposes for which the data is to be used;
• The class of persons to whom the data may be transferred; and
• The individual’s rights to access his personal data, to challenge its accuracy, and to rectify it.

For details on how to prepare a PICS, organisations may refer to “Guidance on Preparing Personal Information Collection Statement and Privacy Policy Statement”.

Label clearly mandatory and optional fields. If an organisation provides personal data by online form, as well as paper forms, the types of personal data thereby collected should be the same unless there is good justification. In particular, mandatory items and optional items to be collected should be clearly labelled and users should be allowed to choose to provide or not to provide personal data of each kind.

Use of cookies and online behavioural tracking. If a website uses cookies, it is good practice to explicitly state what kind of information (regardless of whether personal data) is being collected from the cookies. If a website deploys third-party cookies, regardless of whether any personal data is involved, it should state that the third-party will have access to such information. Such information collected, to which the information may be transferred and for what purposes.

If acceptance of the use of cookies is mandatory, this should be stated clearly on the website. If acceptance of the use of cookies is voluntary, users should be provided with such option with clear information on what the consequences will be if users decide not to accept cookies (for example, not accepting session cookies may affect the proper functioning of website).

Where online tracking is involved, data users should be careful of the Law and transparency required in the “Online Behavioral Tracking” Information Leaflet.

DPP2 – Accuracy and Duration of Retention

Accuracy of personal data

DPP2(1) requires a data user to take all reasonably practicable steps to ensure the accuracy of the personal data that he collects. This does not only apply to the accuracy of the personal data collected via websites, appropriate and practicable steps should still be taken to ensure that the data is accurate.

For example, a “double confirmation” sending a verification email message to the reported email address to confirm that the address has been entered correctly may be required to ensure that any subsequent messages are sent to the correct address. Online verification is not feasible, offline verification may need to be performed.

Duration of personal data retention

DPP2(2) requires a data user to take all reasonably practicable steps to ensure that the personal data that he collects is not kept longer than is necessary for the purpose for which it is or is to be used. In addition to having a policy setting out the intention period of the data, it is important to have a mechanism to ensure that both online and offline copies of the personal data concerned are erased after the intention period.

The engagement of data processors

Furtherehr, DPP2(3) provides that where a data user engages a data processor, whether within or outside Hong Kong, to process personal data on the data user’s behalf, the data user must ensure that the data processor is capable of preventing any personal data transferred to the data processor from being used for any purpose other than that for which it is transferred for processing of the data. Organisations may refer to the information leaflet “Outsourcing the Processing of Personal Data to Data Processors” for more details.

DPP3 – Use of Personal Data

Display of personal data through the Internet

DPP3 provides that personal data should not be used for a purpose unless it has been consented to. In general, and voluntary consent is obtained from the data subject or his “relevant person” as defined under the Ordinance.

Displaying or disclosing personal data through the Internet should be kept to a minimum. If it is necessary, the data user should consider whether he needs any other measures to prevent any personal data transferred to the data processor from being used for any purpose other than that for which it is transferred for processing of the data. Organisations may refer to the information leaflet “Outsourcing the Processing of Personal Data to Data Processors” for more details.

• State at the time of collection that the personal data will be displayed. If personal data to be collected may later be displayed through the Internet or elsewhere, this intention should be made clear in the question on or before collecting his personal data. An example could be an Internet-based service which makes available, through the Internet, private users’ details to parents online. At the time of collecting personal data, the data user should have informed the parent that his personal data may be displayed through the Internet should be prepared. Otherwise, if the display of the data in this way, the organisation must obtain express consent from the tutors.

• The personal data is not kept longer than is necessary for the personal data.

• The personal data is not kept longer than is necessary for the personal data.

DPP4 – Security of Personal Data

Securing the storage and transmission of personal data

Administrative and technical measures should be taken to ensure that security precautions, the level of which should be commensurate with the sensitivity of the personal data, should be adopted. This could result from an act of the Internet, so organisations should be careful in ensuring that security measures are implemented for the storage and transmission of personal data.

• Implement a top-down, Privacy by Design approach. A top-down approach is required for organisations to ensure that security measures are put in place to achieve that protection. A Privacy by Design approach should be adopted to ensure that personal data protection is built in as an integral part of any system at the feasibility stage and not as an afterthought.

• Carry out risk assessment. Not all personal data stored online or transmitted through the Internet is kept to the same degree of protection. The appropriate degree of protection depends on the sensitivity and volume of the personal data involved. On this basis, risk assessments should be carried out regularly for the various kinds of personal data that are stored or transmitted through the Internet. Organisations should then regularly review and revise appropriate policies, guidelines, and measures to ensure the protection of personal data from any improper use by third parties. Organisations should be mindful that the improper use of any displayed personal data by third parties. Organizations should be required to implement appropriate policies, guidelines, and measures to protect the confidentiality and integrity of the personal data in their systems. Such measures will also need to ensure the accuracy of the personal data is not kept longer than is necessary for the purpose.

Policy on the handling of personal data

• Set policies on the handling of personal data. Section 56 of the Ordinance provides that an organisation must have policies, guidelines, and procedures to protect the personal data in its possession or under its control, and ensure that the personal data is kept secure. An organisation should set policies, procedures and guidelines on the handling of personal data and its staff should be regularly reminded to observe the same. Similar liability exists under section 62(2) of the Ordinance. An organisation is responsible for ensuring that an engaging an agent to handle personal data on its behalf, the agent must adopt appropriate policies, guidelines, and procedures. An organisation should assess or examine the system that the service provider has implemented to protect personal data and should make sure that the service provider takes place adequate security measures and practices.

Related information


Guidelines for Data Users on the Collection and Use of Personal Data through the Internet

April 2014

Guidelines for Data Users on the Collection and Use of Personal Data through the Internet

April 2014

Guidelines for Data Users on the Collection and Use of Personal Data through the Internet

April 2014

Guidelines for Data Users on the Collection and Use of Personal Data through the Internet

April 2014

Guidelines for Data Users on the Collection and Use of Personal Data through the Internet

April 2014
Collecting personal data through the Internet

DPP(1) sets out the information that a data user has to provide to an individual on or before collecting personal data from him online in the course of providing his personal data are supplied with the information required by DPP(2).

Use of cookies and online behavioural tracking. If a website uses cookies, it is good practice to explicitly state what kind of information (regardless of whether personal data is involved) is stored in the cookies. If a website deploys third-party cookies, regardless of whether any personal data is involved, it should state the information which cookies collect, to whom the information may be transferred and for what purposes.

If the acceptance of cookies is mandatory, this should be stated clearly on the website. If acceptance of the use of cookies is voluntary, users should be provided with such option with clear information on what the consequences will be if users decide not to accept cookies (for example, not accepting session cookies may affect the proper functioning of websites).

Where online tracking is involved, data users should advise individuals of the lack and transparently provide links to PICS.

Accuracy of personal data

DPP(2) requires a data user to take all reasonably practicable steps to ensure that the personal data that he collects are accurate and complete. For international purposes, the personal data must be as accurate and complete as is necessary for the purpose for which it is to be used. In addition to having a policy setting out the intention period of the personal data, a data user should also establish a mechanism to ensure that both online and offline copies of the personal data concerned are erased after the intended period.

Limit the purpose of use

State at the time of collection that personal data will be displayed. If a data user wishes to make personal data publicly available on or before collecting personal data from individuals, it should be clearly stated.

Duration of personal data retention

DPP(2) requires a data user to take all reasonably practicable steps to ensure that the personal data collected remain necessary for fulfillment of the purpose for which it is to be used. In addition to having a policy setting out the intention period of the personal data, a data user should also establish a mechanism to ensure that both online and offline copies of the personal data concerned are erased after the intended period.

Security of Personal Data

Securing the storage and transmission of personal data

Data users should take all reasonably practicable steps to implement security precautions, the level of which should be commensurate with the seriousness of the consequences that could result from a data breach. Security is generally weak on the Internet, so to protect personal data from unauthorised access, security measures are implemented for the storage and transmission of personal data.

Implement a top-down, Privacy by Design approach. A top-down approach is required for organisations to ensure that personal data protection is built into an integral part of systems and procedures as a default. Appropriate measures are put in place to achieve that protection. A Privacy by Design approach should be adopted to ensure that personal data protection is built into an integral part of any system at the feasibility stage as yet as an afterthought.

Carry out risk assessment. Not all personal data stored online should be handled using the same degree of protection. The appropriate degree of protection depends on the sensitivity and volume of the personal data involved. On this basis, risk assessments should be carried out regularly for the various kinds of personal data that are stored or transmitted through the Internet. Organisations should then regularly devise and review appropriate policies, guidelines and procedures to protect personal data.

Set policies on the handling of personal data. Section 65(2) to 65(3) of the Ordinance place liability on the employer of the data user for any act of his employees done in the course of employment, unless the employer can provide evidence that it has taken all reasonably practicable to prevent the employee from incurring the requirements under the Ordinance. Hence, an organisation should set policies, procedures and guidelines on the handling of personal data and staff should be regularly reminded to observe the same. Similar liability exists under section 65(2) of the Ordinance where an organisation is engaging an agent to handle personal data on its behalf. The agent should observe the same principles. The organisation should assess or examine the systems that the service provider has implemented to protect personal data and consider whether these place adequate security measures and practices.

Consider the use of technological safeguards. If an organisation hosts an application or maintains a database which allows access to personal data online, it should ensure that personal data from unauthorised access, and update such measures regularly to tackle evolving security risks. Examples of such measures are listed below:

- Encrypt personal data being transmitted to prevent unauthorised interception or access. For example, for storing the master key in the Internet, it should be protected by access controls, encryption and/or other appropriate measures to prevent unauthorised access.

- Controls on password complexity, re-tries and issues should be implemented to prevent wrong password being used.

- A properly configured firewall should be used to prevent personal data from being sent to unauthorised parties. Where appropriate, servers or databases holding or receiving personal data should be protected by firewalls. Data users should also ensure that Internet users are not allowed direct access to the personal data.

Consider the use of technological safeguards. If an organisation hosts an application or maintains a database which allows access to personal data online, it should ensure that personal data from unauthorised access, and update such measures regularly to tackle evolving security risks. Examples of such measures are listed below:

- Encrypt personal data being transmitted to prevent unauthorised interception or access. For example, for storing the master key in the Internet, it should be protected by access controls, encryption and/or other appropriate measures to prevent unauthorised access.

- Controls on password complexity, re-tries and issues should be implemented to prevent wrong password being used.

- A properly configured firewall should be used to prevent personal data from being sent to unauthorised parties. Where appropriate, servers or databases holding or receiving personal data should be protected by firewalls. Data users should also ensure that Internet users are not allowed direct access to the personal data.

- Secure on the handover of personal data. Section 65(1) of the Ordinance places liability on the employer of the data user for any act of his employees done in the course of employment, unless the employer can provide evidence that it has taken all reasonably practicable to prevent the employee from incurring the requirements under the Ordinance. Hence, an organisation should set policies, procedures and

- Limits personal data retention. The Commissioner has published a Guidance Note on Personal Data Erasure and Anonymisation which is available at www.pcpd.org.hk/eng/publications/files/online_tracking_e.pdf.

- Implement a top-down, Privacy by Design approach. A top-down approach is required for organisations to ensure that personal data protection is built into an integral part of systems and procedures as a default. Appropriate measures are put in place to achieve that protection. A Privacy by Design approach should be adopted to ensure that personal data protection is built into an integral part of any system at the feasibility stage as yet as an afterthought.

- Carry out risk assessment. Not all personal data stored online should be handled using the same degree of protection. The appropriate degree of protection depends on the sensitivity and volume of the personal data involved. On this basis, risk assessments should be carried out regularly for the various kinds of personal data that are stored or transmitted through the Internet. Organisations should then regularly devise and review appropriate policies, guidelines and procedures to protect personal data.

- Set policies on the handling of personal data. Section 65(2) to 65(3) of the Ordinance place liability on the employer of the data user for any act of his employees done in the course of employment, unless the employer can provide evidence that it has taken all reasonably practicable to prevent the employee from incurring the requirements under the Ordinance. Hence, an organisation should set policies, procedures and
Collecting personal data through the Internet

DPP1(3) sets out the information that a data user has to provide to an individual or ask them to submit their personal data as well as the time frame within which they shall provide to an individual on or before collecting personal data. Thus, DPP1(3) requires a data user to take reasonable practicable steps to ensure that individuals providing personal data.

Use of cookies and online behavioural tracking. If a website uses cookies, it good practice to explicitly state what kind of information (regardless of whether personal data or not) is automatically collected and stored in the cookies. If a website displays third-party cookies, regardless of whether any personal data is involved, it should state whether the cookie is used for information about such cookies, to collect, to whom the information may be transferred for what purposes.

If the acceptance of the use of cookies is mandatory, this should be stated clearly on the website. If acceptance of the use of cookies is voluntary, users should be provided with such option with clear information on what the consequences will be if users decide not to accept cookies (for example, not accepting session cookies may affect the proper functioning of websites).

Where online tracking is involved, data users should observe the following points:

• Whether it is obligatory or voluntary for the individual to supply the data, and where it is obligatory, the consequences for failure to supply the data;

• The purposes for which the data is to be used;

• The classes of person to whom the data may be transferred; and

• The individual’s rights to request access to a copy of his personal data, to oppose the processing of the data, and the name or title, and address, of the responsible person to whom such request may be made.

For details on how to prepare a PICS, organisations may refer to “Guidance on Preparing Personal Information Collection Statement and Privacy Policy Statement”.

Label clearly mandatory and optional fields. If an organisation requests personal data by online form as well as paper form, the types of personal data thereby collected should be the same unless there is good justification. In particular, mandatory items and optional items to be collected should be clearly labelled and users should be allowed to proceed even if they do not want to answer the mandatory items.

Use of cookies and online behavioural tracking. If a website uses cookies, it good practice to explicitly state what kind of information (regardless of whether personal data or not) is automatically collected and stored in the cookies. If a website displays third-party cookies, regardless of whether any personal data is involved, it should state whether the cookie is used for information about such cookies, to collect, to whom the information may be transferred for what purposes.

The engagement of data processors

Furthermore, DPP2(3) provides that where a data user engages a data processor, whether within or outside Hong Kong, to process personal data on the user’s behalf, the data processor must ensure that measures are put in place to prevent any personal data transferred or disclosed to the third party is used in a manner that is not necessary for the purpose of processing the data. Organisations may refer to the information leaflet “Outsourcing the Processing of Personal Data to Data Processors” for more details.

DPP2 – Accuracy and Duration of Retention

Accuracy of personal data

DPP2(3) requires a data user to take reasonable practicable steps to ensure the accuracy of the personal data collected. This means that a data user should not only promptly check the accuracy of the personal data collected, but that they must also provide appropriate and practicable steps to correct any errors in the data. For example, a “double confirmation” sending a verification email message to the reported email address of the address that the address has been entered correctly, may be required to ensure that any subsequent messages are sent to the correct address. If verification is not feasible, offline verification may need to be performed.

Duration of personal data retention

DPP2(2) requires a data user to take all reasonably practicable steps to ensure that the personal data to be held is necessary for the purpose for which it is to be used. In addition to having a policy setting out the intention period of the personal data, it is also necessary to establish a mechanism to ensure that both online and offline copies of the personal data concerned are erased after the expiration of this period. For example, if a website uses cookies, it good practice to explicitly state what kind of information (regardless of whether personal data or not) is automatically collected and stored in the cookies. If a website displays third-party cookies, regardless of whether any personal data is involved, it should state whether the cookie is used for information about such cookies, to collect, to whom the information may be transferred for what purposes.

The engagement of data processors

Furthermore, DPP2(3) provides that where a data user engages a data processor, whether within or outside Hong Kong, to process personal data on the user’s behalf, the data processor must ensure that measures are put in place to prevent any personal data transferred or disclosed to the third party is used in a manner that is not necessary for the purpose of processing the data. Organisations may refer to the information leaflet “Outsourcing the Processing of Personal Data to Data Processors” for more details.

DPP3 – Use of Personal Data

Display of personal data through the Internet

DPP3 provides that personal data should not be used for a purpose unless prior informed consent, i.e. express and voluntary consent is obtained from the data subject or his/her “relevant person” as defined under the Ordinance. Checking or displaying personal data through the Internet may constitute the use of personal data. Hence, in order to comply with the requirements under DPP3, organisations should ensure that the display or handling personal data is as limited as possible. The display of personal data is only limited to the specific purposes mentioned. Where the use of the personal data is directed marketing is not allowed, it should be clearly stated.

DPP4 – Security of Personal Data

Securing the storage and transmission of personal data

DPP4(1) requires a data user to take all reasonably practicable steps to implement security precautions, the level of which should be commensurate with the seriousness of the personal data involved. For example, engaging an agent to handle personal data on its behalf could result from a breach of data security. Hence, an organisation should examine or examine the systems that the service provider has implemented to protect personal data and its security. This includes the organisation to place adequate security measures and practices.

Consider the use of technological safeguards. If an organisation hosts an application or maintains a database which allows access to personal data online, it should implement security measures to prevent unauthorised access to personal data from unauthorised access, and update such measures regularly to tackle evolving security risks. Examples of such measures are listed below:

• Encrypt personal data being transmitted to prevent unauthorised interception or access.

• Use strong passwords. For example, in the Internet, it should be protected by access controls, encryption and/or other appropriate measures to prevent unauthorised access.

• Controls on password complexity, re-tests and issues should be implemented to prevent password from being compromised.

• A properly configured firewall should be used to prevent unauthorised access to certain personal data.

• Where appropriate, servers or databases holding or receiving personal data should be password protected. This is to prevent unauthorised access by website visitors by guessing the URL.

• Set policies on the handling of personal data. Section 30(4) of the Ordinance requires the data user to develop policies on the handling of personal data. These policies should be reviewed and updated regularly. The policies should be designed to ensure that all personal data is handled in compliance with the Ordinance.

Guidelines for Data Users on the Collection and Use of Personal Data through the Internet. April 2014

Guidelines for Data Users on the Collection and Use of Personal Data through the Internet. April 2014

Guidelines for Data Users on the Collection and Use of Personal Data through the Internet. April 2014

Guidelines for Data Users on the Collection and Use of Personal Data through the Internet. April 2014

Available at www.pcpd.org.hk/english/publications/files/GN_picspps_e.pdf

Available at www.pcpd.org.hk/english/publications/files/GN_picspps_e.pdf

Available at www.pcpd.org.hk/english/publications/files/GN_picspps_e.pdf

Available at www.pcpd.org.hk/english/publications/files/GN_picspps_e.pdf

The Commissioner has published a Guidance Note on Personal Data Security and Assurance which is available at www.pcpd.org.hk/english/publications/files/GN_picspps_e.pdf

Available at www.pcpd.org.hk/english/publications/files/GN_picspps_e.pdf

For example, if the data subject is a minor, an organisation may obtain the prescribed consent from his parent. See the definition of “relevant person” as defined under the Ordinance.
• Do not store or request users to upload file containing personal data in webserver without proper protection such as access control and encryption. Access to such databases page or page where personal data is collected, e.g. a membership registration page or a customer account page. The link should be clearly labelled, for example, with a heading such as “Privacy Policy” or in the form of a button or icon carrying with similar meaning.

• Make the privacy policy statement easy to access. Everyone should be made aware of the importance of respecting the data rights of individuals, both as a moral obligation and as a legal requirement. All personnel involved in the handling of personal data should be adequately trained in understanding the requirements of the Ordinance and the compliance procedures in place.

• Set an action plan for data breach handling. Data leakage on the Internet can spread quickly and widely, and where the leakage may cause irreversible damage to the reputation of an organisation. A transparent and fast breach handling system should therefore be in place to cut out a clear action plan to be followed to contain any breaches, and to mitigate the damage caused to the data subjects concerned.

The engagement of data processors (DPP4) provides that if a data user engages a data processor, whether within or outside Hong Kong, to process personal data, the data user must adopt contractual or other means to prevent unauthorised or accidental access, processing, erasure, loss, or use of the data transferred to the data processor.

For details on how to prepare a PPS, organisations may refer to “Guidance on Preparing Personal Information Collection Statement and Privacy Policy Statement”.

DPP6 – Access to Personal Data

Under the Ordinance, individuals have the right to request access to, and correction of, their personal data held by an organisation. There are different situations in which an individual may want to access his or her personal data, such as to confirm its accuracy, to verify data collection practice. Special care is needed when handling personal data of children. The language relating to personal data management should be straightforward and avoid technical terms for easy understanding of the child.

DPP7 – Transparency of Policies and Practices

Openness of the organisation's personal data privacy policy

Organisations engaged in direct marketing activities using personal data must comply with Part VI A of the Ordinance regarding direct marketing activities. Organisations should refer to the “New Guidance on Direct Marketing” for more details.

DPP1 – Purpose and Manner of Collection

Adequate but not excessive personal data collection provides that personal data shall be collected by the data user for the purposes for which the data is used, and not for any other purposes. For example, if an online purchase or delivery is to be made, generally it would not be necessary to collect the credit card number or residential address of a customer. Normally, date of birth should not be requested when all that is needed is the age of the individual for tracking purposes. In any case, the same information should not be collected unless it is necessary over a certain age. Another example is that the gender of an individual should only be requested if it is relevant to the individual's identification, and not for any other purposes.
Do not store or request users to upload file containing personal data in webserver without proper protection such as access control and encryption, otherwise the user and/or the webserver may be compromised. Contemporary social networking sites are powerful enough to spread ill-liked URLs.  
Consider installing a data loss prevention (DLP) system which, among other things, blocks access to suspicious URLs. Internet communications for unauthorised disclosure of personal data.  
If multiple server roles or applications are hosted on a single server, cross-application access rights and/or cross-application data transfer is elected by an individual for the personal data to be tested to prevent unauthorised access to personal data from one application to another.  
Consider the use of privacy-enhancing technologies whenever possible to protect personal data privacy. Privacy-enhancing technologies are measures that help to minimize the risk of personal data exposure, such as encryption, or hashing to mask data confidentiality, where possible it is desirable to protect search engines from indexing websites, a customer agreement page. The link should be prominently displayed, e.g. a membership registration page or a customer agreement page. The link should be clearly labelled, for example, with a heading such as “Privacy Policy” or in the form of a button or icon carrying with similar meaning.  
Make the privacy policy statement easy to access. Every employee should be made aware of the importance of respecting the data rights of their fellow employees and the website pages on which personal data is collected, e.g. a membership registration page or a customer agreement page. The link should be clearly labelled, for example, with a heading such as “Privacy Policy” or in the form of a button or icon carrying with similar meaning.  
State the privacy policy clearly. The PPS should inform users of the kind of personal data held by the organisation and the main purposes for which the personal data is or is to be used. It may contain information about other matters relating to the privacy of personal data, such as the use, if any, of cookies by the organisation to track its visitors, the organisation’s policy on direct marketing, and its security and retention policies in relation to personal data. For details on how to prepare a PPS, organisations may refer to “Guidance on Preparing Personal Information Collection Statement and Privacy Policy Statement”.  
PPPs – Access to Personal Data  
Under PPPs, all individuals have the right to request access to, and correction of, their personal data held by an organisation. There is no difference in treatment, no low or high status of the user with, i.e. the transmission of the user’s personal data, an appropriate alert should be given to the individual about the risks prior to the transmission.  
Avoid using known personal data for authentication. It is possible that the personal data that is obtained by third parties relatively easily, such as date of birth, ID card number or phone number, should be obtained by third parties relatively easily, such as date of birth.  
DPPs – Transparency of Policies and Practices  
Openness of the organisation’s personal data policy  
DPP5 stipulates openness by organisations about their policies and practices in relation to personal data. An organisation with a website should make its privacy policy statement (“PPS”) either accessible or linkable.  
To provide more reliable contact channels, the organisation should disclose clearly its name, physical address, contact person, telephone number and/or fax number, e-mail address, in addition to its web address and/or e-mail address, in the “About us” and/or “Contact us” section.  
Promote a privacy-aware culture in the workplace. Every employee should be made aware of the importance of respecting the data rights of their fellow employees and the website pages on which personal data is collected, e.g. a membership registration page or a customer agreement page. The link should be clearly labelled, for example, with a heading such as “Privacy Policy” or in the form of a button or icon carrying with similar meaning.  
Guidance for Users on the Collection and Use of Personal Data through the Internet  
Introduction  
Operating online businesses or services, whether by commercial enterprises, non-governmental organisations or individuals, the use of personal data is inevitable. In many cases, offering such transactions involves the collection of personal data.  
The Personal Data (Privacy) Ordinance (the Ordinance) provides for data protection principles (“DPPs”), which set out fair information practices on how personal data should be handled when used by data users. The data user is defined as a person to whom personal data is or is to be used. It may contain information about other matters relating to the privacy of personal data, such as the use, if any, of cookies by the organisation to track its visitors, the organisation’s policy on direct marketing, and its security and retention policies in relation to personal data.  
In December 2011, the Office of the Privacy Commissioner for Personal Data (PCPD) published the first edition of “Guidance for Data Users on the Collection and Use of Personal Data through the Internet” (the Guidance). The Guidance has proved to be very useful in guiding data users in complying with the Ordinance while engaging in the collection, display or transmission of personal data through the Internet.  
DPP1 – Purpose and Manner of Collection  
Adequate but not excessive personal data collection  
It is important to understand that the personal data that is obtained by third parties relatively easily, such as date of birth, ID card number or phone number, should be obtained by third parties relatively easily, such as date of birth.  
Under DPPs, all individuals have the right to request access to, and correction of, their personal data held by an organisation. There is no difference in treatment, no low or high status of the user with, i.e. the transmission of the user’s personal data, an appropriate alert should be given to the individual about the risks prior to the transmission.  
Avoid using known personal data for authentication. It is possible that the personal data that is obtained by third parties relatively easily, such as date of birth, ID card number or phone number, should not be used as an initial or password or verification code.