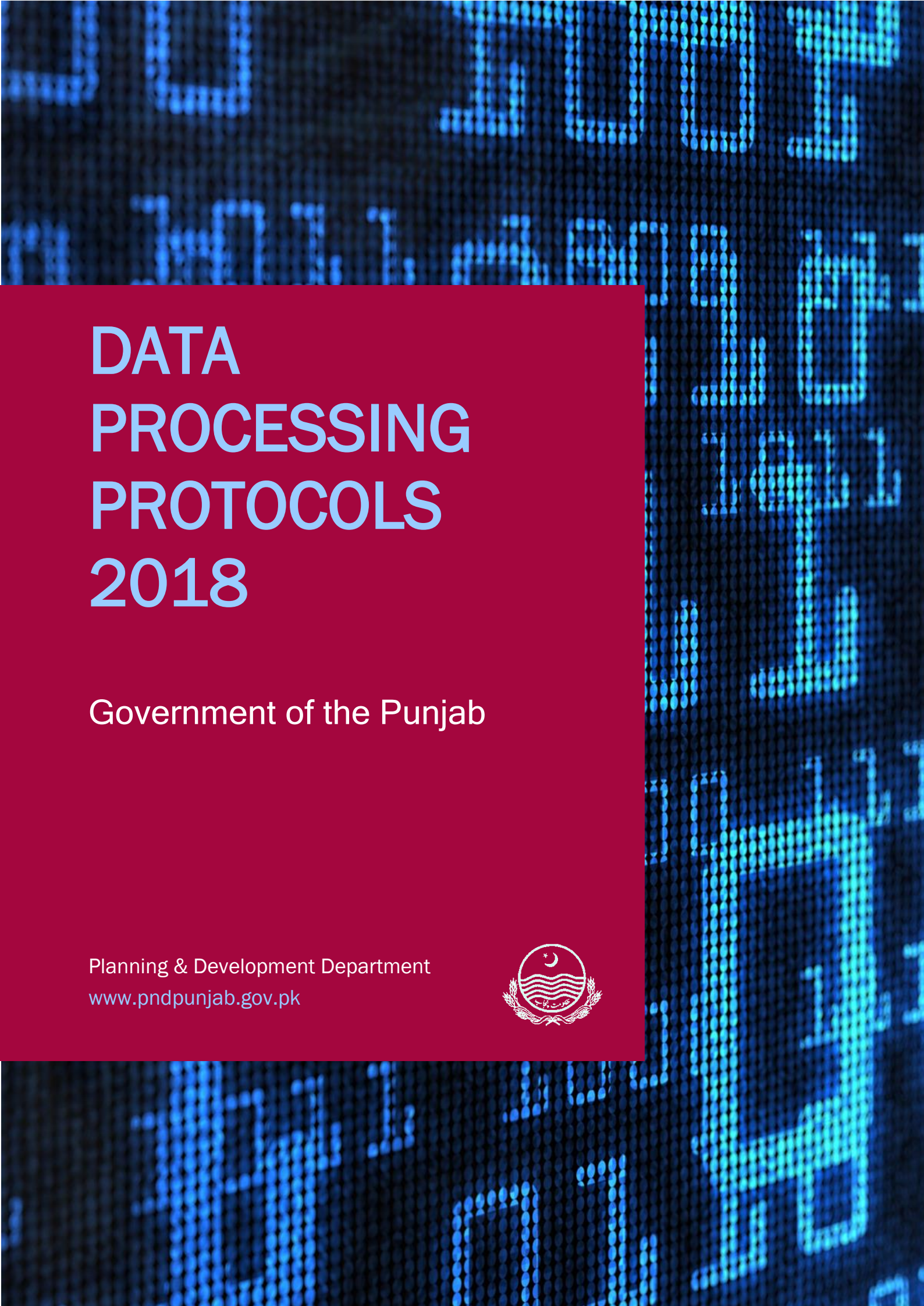

DATA PROCESSING PROTOCOLS 2018

Government of the Punjab

Planning & Development Department
www.pndpunjab.gov.pk

DATA PROCESSING PROTOCOLS 2018

Government of the Punjab

Planning & Development Department

(Governance & IT Wing)

These Protocols relate to the handling of Personal Data by the departments and attached bodies of Government of the Punjab.

The Protocols are envisaged to be a living document and shall be reviewed and amended periodically. We welcome feedback and suggestions from all the organizations and individuals for further improvement of the document. Queries and feedback may be sent to:

Chief (Governance & Information Technology): chiefit@pndpunjab.gov.pk
Planning Officer (Information Technology): poit@pndpunjab.gov.pk

PREFACE

The Data Processing Protocols were developed by the Governance & IT Wing of the Planning & Development Department, with the expertise of Ms. Lucia Bird, Legal & Policy Adviser to Planning & Development Department.

These Protocols relate to the handling of Personal Data by the departments, subsidiary authorities, autonomous bodies and bodies corporate in which the Government of the Punjab holds over 50% shares (Organizations). Certain components of the Protocols, including the security provisions, apply to all Confidential Data handled by the Organizations.

The purpose of these Protocols is to support Organizations in designing and implementing systems and procedures which ensure that Personal and Confidential Data is processed securely, in line with best practice and in a manner which respects individuals' right to privacy.

The Protocols are based on universal principles of secure data processing and are a product of a co-creation process, reviewed by Chief (Governance & IT) and Member (IT) before receiving the approval of Secretary and Chairman P&D Board. In preparation of the Protocols a number of consultative sessions were conducted with various government agencies to identify needs and seek suggestions.

A high level meeting convened by Governance & IT Wing of P&D Department on 11th May 2018 is particularly remarkable. The meeting, chaired by Chairman P&D Board, was attended by relevant officers from many government departments and attached bodied besides the Members of P&D Board. Based on valuable feedback of the participants of this session, the draft was improved and again circulated to all the department / agencies for comments before finalization.

The Protocols are envisaged to be a living document and shall be reviewed and amended periodically.

CONTENTS

1. Introduction

These Data Processing Protocols ("Protocols"), developed pursuant to the Federal Government Internet and Emails Policy, constitute the first step in ensuring the data governance of the Government of Punjab ("GoP") is in line with best practice. It is envisaged that further guidance shall be published pursuant to these Protocols, in due course. These Protocols shall be reviewed and updated regularly and in any event annually, to ensure they are in line with the changing regulatory framework.

These Protocols constitute the minimum standards Organizations should implement to protect the Personal and Confidential Data they process. Organizations should develop more detailed and tailored protocols for their own processes – and are free to set higher standards of protection. Periodic independent third party audits of IT and data security measures are recommended for all Organizations.

Organizations shall have a transitional period of six (6) months in which to implement the requirements of these Protocols. After the transitional period compliance with these Protocols is compulsory. Capacity building initiatives should seek to ensure that all Organization staff are able to comply with these Protocols by the end of the transitional period.

2. Why do we need these Protocols?

Leaks of data harm the reputation of Government and the trust of the public in Government institutions. Enhanced data processing protocols support government institutions in safeguarding the data they process, minimizing the risk of leaks or hacks.

Article 14(1) of the Constitution of the Islamic Republic of Pakistan 1973 enshrines the right to privacy as a fundamental right, stating that "the dignity of man and, subject to law, the privacy of home, shall be inviolable". Pakistan is signatory to a number of international conventions protecting the privacy of individuals.[1] GoP is taking steps to ensure the public's right to privacy is being respected by ensuring it is only collecting personal data when it is necessary in the pursuance of its functions and in order to provide services, and processing data with appropriate concern to access and safety.

3. Scope

These Protocols relate to the handling of Personal Data (defined below), by GoP departments, subsidiary authorities, autonomous bodies and bodies corporate in which the GoP holds over 50% shares ("Organizations"). Certain elements of the Protocols, including the security provisions, apply to all Confidential Data (defined below) handled by Organizations.

[1] Including: The International Covenant on Civil and Political Rights (signed April 2008, ratified June 2010), Article 17; The Cairo Declaration on Human Rights in Islam (signed August 1990) Article 18.

The purpose of these Protocols is to support Organizations in designing and implementing systems and procedures which ensure that Personal and Confidential Data is processed securely, in line with best practice and in a manner which respects individuals' right to privacy.

4. Audience

These Protocols should be read by senior management and brought to the attention of all employees that process any Personal Data. It is envisaged that this will include the majority of employees. Organizations should require employees to confirm in writing that they have read and understood the Protocols and agree to comply with them.

5. What is Personal Data?

Personal Data is information which, either on its own or in combination with other information the Organization holds, can be used to identify a living individual.

This will include, but not be limited to, name, address, and CNIC. The medium through which the personal data is held (i.e. whether electronically or on paper) is irrelevant – these Protocols apply equally to Personal Data held on a computer or in a notebook.

6. Definitions

a. **Confidential Data** means Personal Data and any information which is not in the public domain;
b. **Data controller** or '**controller'** means the natural or legal person (i.e. corporate entity or individual) which, alone or jointly with others, determines the purpose of the processing and the manner of the processing of Personal Data (here the purpose is particularly important);
c. **Data processor** or **'processor'** means the natural or legal person (i.e. corporate entity or individual) which processes Personal Data on behalf of the data controller (i.e. on the instructions of);
d. **Data subject** means the individual or person to whom the data are related;
e. **Fair Processing Information** means (i) the purpose of processing; (iii) whether the data will be shared with any other entities, and if so with whom; (iv) the name and address of the data controller;
f. **Personal Data** has the meaning given to it in paragraph 5 above;
g. **Processing** means any handling of Personal Data, or Confidential Data, as appropriate (whether or not by automated means) including but not limited to collecting, storing, organizing, altering, using, sharing etc.;
h. **Protected Personal Data** means Personal Data which, (i) if released, would put the relevant individual at significant risk of harm or distress (this includes credit or debit card details, fingerprints or tax records); or (ii) relates to 1000 or more individuals that is not in the public domain;

i. **PTRI Act** means The Punjab Transparency and Right to Information Act 2013; and
j. **Sensitive Personal Data** means Personal Data revealing ethnicity or race, political opinions, religious or philosophical beliefs, trade union membership, data concerning health or a natural person's sex life or sexual orientation, or criminal convictions or charges.

Case Study: Data Controllers and Data Processors

If an Organization hires a company to collect data which includes Personal Data and build a data set which the Organization will use in order to fulfill its functions, the Organization is the Data Controller and the company is the Data Processor. The company will be processing the Personal Data, however only in accordance with the instructions of the Organization.

A written agreement between the controller and processor should include a representation from the processor that it will only process the Personal Data pursuant to the controller's instructions.

7. Mapping Data

All Organizations should conduct an audit to identify (i) what Personal Data they hold; (ii) where this Personal Data is stored; (iii) whether they are providing the public with Fair Processing Information; and (iv) the current data security measures in place. This audit will make sure Organizations are well placed to implement these Protocols and will help Organizations identify where they are collecting Personal Data that they don't need, and amend processes accordingly. Organizations should conduct information audits regularly, and at least annually.

8. Conditions for Processing Personal Data

Organizations should ensure Personal Data is:

1) processed fairly, transparently, and in line with all applicable legislation;
2) processed for limited, specifically stated purposes;
3) processed in a way that is adequate, relevant and not excessive in relation to the purpose for which it is processed;
4) kept accurate;
5) kept for no longer than is absolutely necessary;
6) processed in accordance with the rights of the data subject, including their right to privacy; and
7) kept safe and secure.

The Organization which is the data controller shall be accountable for ensuring the Personal Data is processed in line with the conditions set out at 1-7 above.

9. Categories of Personal Data

Within Personal Data there are different categories of data, Protected Personal Data and Sensitive Personal Data, which are of greater sensitivity and liable to cause greater harm to the individual if released. Consequently both require enhanced security standards. In addition, Sensitive Personal Data can only be processed if additional conditions are met. These conditions are set out in paragraph 10 (*Purpose of Processing*) below.

10. Purpose of Processing

Organizations should only be processing Personal Data where the processing:

i. is necessary for fulfilling the Organization's function, as set out in the Provincial Rules of Business or National or Provincial Legislation; or
ii. is necessary for fulfilling a task in the public interest (when the underlying task, power or function is set out in law); and
iii. the processing is proportionate and there is no practical less intrusive alternative.

Organizations should only process Sensitive Personal Data, where it is absolutely necessary in order to protect the vital interests of the data subject or for reasons of substantial public interest. 'Substantial public interest' includes public health, establishing or defending legal claims and crime prevention. Where Organizations collect Sensitive Personal Data, access should be extremely restricted and security precautions high.

Organizations should only process the Personal Data for the purpose for which it was collected. Organizations cannot use the Personal Data for a different purpose unless that purpose is authorized or required by law, it is directly related to the purpose for which the Personal Data was collected, or the data subject authorizes the different use.

11. Information to be given to the Data Subject

11.1 Fair Processing Information

In order for the processing to be fair, when collecting Personal Data Organizations must ensure data subjects are provided with Fair Processing Information, i.e.

i. the purpose of processing;
ii. whether the data will be shared with any other entities, and if so with whom; and
iii. The name and address of the data controller.

It is best practice to have a comprehensive document setting out this information, a 'Privacy Policy' or 'Personal Data Statement', on each Organization's website. A template Privacy Policy is set out at Annex D. This should be tailored to the organization and then posted on the website under a clear tag, e.g. 'Privacy' or 'Your Personal Information'.

Organizations should review the Privacy Policy published on their website regularly and at least every four months, or when new projects are launched, and updated accordingly. This applies

both to Personal Data Organizations collect directly from individuals and to Personal Data Organizations collect from another source, e.g. if it is transferred by a different Organization.

In addition, when an Organization is collecting Personal Data from individuals it should consider whether it would be appropriate to provide Fair Processing Information, e.g. if an Organization designs an app which requires the public to login by entering their name, address and telephone number, prior to entering the information the individual should be provided with Fair Processing Information. It will be appropriate to provide individuals with Fair Processing Information in the majority of cases.

11.2 Websites - Privacy Notice

Most, if not all, Organizations collect Personal Data from users of their websites and mobile apps, through feedback or suggestion platforms, the use of cookies and other more specific functions.

Consequently, all Organizations should include information about the data collected on the website in the Privacy Policy published on their websites.

In addition, Organizations should review whether the Personal Data collected from individuals on websites is appropriate and not excessive. For example, where a feedback form is provided, although it may be necessary to request the email or telephone number in order to be able to contact the person, it may not be necessary to request their address if feedback is unlikely to be by post. The template Privacy Notice at Annex D also addresses Person Data collected on websites. Please amend according to your website's functions.

12. Keeping Data Secure

Please note that these provisions apply to all Confidential Data held by Organizations. Confidential Data means (i) Personal Data; and (ii) any information held by the Organization which is not in the public domain.

All Organizations should have properly configured Network Infrastructure and a certified Network/System administrator(s). This Network Administrator is responsible for ensuring that each Organization shall purchase and implement licensed antivirus software with outbreak support. The anti-virus software should be configured to download the latest virus definition files (DAT files) daily from the internet at night, and send automatic notifications to the Network Administrator in this regard.

All Organizations should have hardware or software firewall installed and configured to protect the network from unauthorized access. All electronic traffic must be routed through this centrally monitored firewall. For further details regarding network security provisions, please refer to Annex E ("Departmental Security Manual") of the Federal E-mails and Internet Policy.

12.1 Access

Access to Confidential Data should be limited to employees that need to process the data in order to fulfill their professional tasks. Where Confidential Data is held on systems with access controls, additional technological controls should prevent the copying of the Confidential Data onto unsecured documents. Access to Confidential Data in archived or historical systems should also be limited by necessity. When logging into any database, staff must do so utilizing their personal user account. Using any other user's account, or the administrative or services account, is prohibited.

Where Organizations have data centers or server rooms, access to these should be restricted to employees who have clearance to work there and strictly require such access to fulfill their functions. Biometric identification procedures should determine such access and a system should record the date of entry and identity of employee entering. Access records should be regularly reviewed by senior management.

Employees of Organizations should take care to ensure that office visitors, or other unauthorized persons, do not view Confidential Data on PC screens or on paper files left unprotected. Staff should ensure PCs are 'locked' or logged off when left unattended and paper files containing Confidential Data locked away at the end of the day.

Pursuant to the Prevention of Electronic Crimes Act 2016, persons who with dishonest intention gain unauthorized access to or copy any information system or data are liable to pay a fine or suffer imprisonment.[2] Consequently unauthorized access by employees can be sanctioned under law.

12.2 Storage of Data

Organizations are encouraged to operate in secure LAN environments, or to utilize secured shared servers for data storage purposes. In order to ensure the security of Confidential Data and to preserve the institutional memory of Organizations, all data processed within the context of the Organization's functions must be stored on secured repositories rather than on local disks. Access controls to the shared server can be configured to regulate which persons have access to the data - storing the data on shared repositories does not mean it becomes automatically accessible by all employees. It does mean that the Organization can ensure the security of data and retains control over it, even if the relevant employee leaves or seeks to block access.

By implementing IT solutions that create auto-backups from local disks, Organizations can ensure data is automatically hosted on the secure network / server. Where data is collected for Organizations on smart phones or other portable devices, these should be backed up on Organization's servers weekly, or where data collection is sporadic, within three Business Days of the data being collected.

[2] Chapter II, ss.3, 4, 6, 7 The Prevention of Electronic Crimes Act 2016.

12.3 Classification of Data

All Organizations shall classify files into Categories A to D in accordance with paragraph 3.44 ('*Classification of Files*') of The Government of Punjab Manual on Secretariat Instruction. In addition, where files are not Confidential or Secret, but they contain Personal Data, they should be marked 'Official – Sensitive' to indicate that these should be handled with care. This is particularly key where the file includes Sensitive Personal Data or significant volumes of Personal Data.

12.4 Email Usage Policy

All employees should be given an official email address upon joining the Organization and should use only the official email address for all matters relating to their employment, pursuant to the following email usage policy:

A. Use of personal email addresses for work purposes is strictly forbidden and presents a serious data security risk. For the avoidance of doubt, any email address ending in anything other than .gov.pk / .gop.pk does not constitute an official email address.
B. Official emails should be not be used for personal matters; offensive or discriminatory content is strictly forbidden and may be subject to disciplinary proceedings. Please note that Organizations have the right to monitor the official email addresses of their employees and sanction unlawful usage if found.
C. Employees are not permitted to set up auto-forwarding from official emails to third party email addresses.

E-mails should be maintained on the Government mail server for audit/documentary/legal purposes for 180 days, unless required for longer.

12.5 Remote Access

Staff should be aware that the Wi-Fi network used to remotely access the Organizations systems should be secure and encrypted, and any machine used to access the network should have up-to-date anti-virus and anti-spy software. Remote access of Organization's data repositories through public unsecured networks is not permitted.

12.6 Passwords

Employees should comply with the following password requirements to protect PCs or any devices containing any Confidential Data:

A. Passwords should be at least 8 characters.
B. Different datasets should be protected by different passwords. One single password should not be used to protect a number of devices and databases.
C. Standard or default passwords must be changed immediately.
D. Passwords should include upper and lowercase letters, numbers and symbols and should not be easily guessable. Staff should therefore avoid biographical information, letter or number sequences and repetition.

E. Passwords should be changed on a regular basis. Staff PCs should be configured to prompt a password change at least every three (3) months.
F. Passwords should not be shared with any other person, be they an employee or a non-professional relationship.

12.7 Laptops and other Mobile Storage Devices

Organizations should seek to ensure that all employees are provided with official laptops and other devices to avoid employees using personal equipment. Where employees use personal laptops and other devices, and store Confidential Data locally, this takes the data out of the Organization's domain and thus control. Only software authorized by the nominated network administrator shall be installed on official laptops.

A significant proportion of employees across Organizations use laptops, either issued by the Organization or personal devices, to fulfill their official duties. In addition, the use of USB sticks and other mobile storage devices is widespread. Although these devices facilitate data transfers and can be extremely useful, they are also easy to lose or steal. Organizations should ensure they implement an asset management and tracking system in order to enable the tracing of all mobile storage devices used by Organization employees.

The following steps must be taken to protect the content held on all devices:

a. All laptops, USB sticks and other mobile storage devices ("portable devices") should be password protected. Passwords should meet the standards set out in sub-paragraph 12.6 above.
b. Confidential Data held on portable devices should be regularly backed up to the Organization's servers.
c. All devices capable of sending or receiving viruses should run up-to-date anti-virus and spyware protection. Organizations should disconnect any non-compliant device from the network and bar re-connection until compliance is achieved.
d. When providing portable devices for use by employees, Organizations should ensure that each device is authorized for use by a named employee. This employee is responsible for the physical safeguarding of this device.
e. Portable Devices taken outside the office should be kept secure at all time.
f. Organizations should develop and implement technologies permitting remote deletion of data from portable devices should they be lost or stolen and put in place procedures to ensure early notification of loss and consequent disconnection of the device from the Organization's systems.
g. Delete all data held on portable devices as soon as it is no longer required.

13. Personnel

13.1 Employment Contracts

The Employment Contracts of all employees should include clauses on data protection, stipulating that the employee must comply with the Organizations' Data Processing Protocols,

and including undertakings regarding the unauthorized sharing of data. Standard clauses are provided at Annex E. These should be included in all employee contracts going forwards. Organizations should consider sending these clauses out to all current employees and asking them to sign and return them. At the very least these clauses should be emailed to employees to heighten awareness. These clauses bind employees to comply with these Protocols; any breach may incur disciplinary action.

13.2 Exit Procedures

When employees or temporarily engaged consultants retire, resign or otherwise leave the Organization, their access credentials should be deleted, their name removed from any mailing lists and they should be reminded that any Confidential Data in their possession due to the role they held at the Organization should be deleted or returned to the Organization, in line with their employment contract (see paragraph 13.1 above). All exiting employees and consultants should have an exit interview with a superior in which they return all Confidential Data and confirm in writing that they have wiped all personal devices of Confidential Data.

The same procedures should be followed where an employee is being transferred internally to a different function and no longer requires access to the same Confidential Data.

13.3 Training for New Staff

New staff should be required to complete a brief online training exercise. Access to Personal Data should be contingent on completion of the exercise. Following completion the employee should confirm in writing that they have understood the training, read these Protocols and agree to comply with them. These written declarations should be recorded and stored by the Organization during the tenure of that person's employment and for one year after termination.

13.4 Annual Training and Certification

Organizations should require all staff to complete the training exercise and sign a refreshed declaration annually. Organizations should provide further, more detailed and tailored, training to staff that process Protected Personal Data or Sensitive Personal Data. Training should cover who in the Organization has the authority to share Personal Data with other entities, and which criteria must be fulfilled for the sharing to take place.

13.5 Consultants or other Contract Staff

Personal or Confidential Data should only be shared with consultants or other contract staff pursuant to a written contract which must include stringent confidentiality and data provisions (see Annexes E and F for clauses to include in employee contracts and contracts with third party service providers). Consultants should be asked to complete the training and sign the certification set out at paragraph 13.3 above and made aware of their confidentiality obligations. Exit procedures should ensure all Confidential Data is returned and, unless stipulated otherwise in the contract, further copies destroyed.

14. Sharing Personal Data

Under the Prevention of Electronic Crimes Act 2016, any person who with dishonest intention and without authorization transmits any data is liable to a fine of one hundred thousand rupees or imprisonment.[3]

14.1 Evaluating Requests

Organizations must have in place procedures which support them in evaluating any request to share Personal Data. Organizations should only comply with such requests where the sharing is strictly necessary and in line with (i) internal procedures; and (ii) these Protocols. Organizations' procedures should specify certain persons (by title) within the Organization who are able to authorize sharing of Personal Data.

When evaluating a request, Organizations should ensure that the Personal Data sharing activity they are considering is reasonably in line with their functions as set out in the Rules of Business or other Legislation. Where the data sharing is not reasonably in line with such functions, Organizations should not share the Personal Data unless there is an overriding public interest mandating the disclosure – this will only be the case in extremely limited situations, including crime prevention. Organizations should consider whether anonymized data would be sufficient to fulfill the purpose – anonymisation significantly decreases the risks associated with Personal Data.

Broadly, individuals should be aware that their Personal Data is being, or may be, shared. However, this is not the case where the sharing of the Personal Data is for (i) detecting or preventing crime or apprehending or prosecuting offenders; or (ii) assessing or collecting revenues. This may typically be addressed by ensuring the Personal Data Statement (Template at Annex D) published on the website is comprehensive.

Prior to deciding to share Personal Data, Organizations should consider the following questions, and keep a record of the answers:

i. Does the requesting Organization have in place appropriate data security measures (note that where Protected or Sensitive Personal Data is being shared security should be enhanced)?
ii. Does the requesting Organization have appropriate access limitations?
iii. How will it be shared? Appropriate security for the transfer should be put in place.
iv. What Personal Data needs to be shared? The sharing should be limited to elements of Personal Data required and not done by bulk datasets. E.g. if another Organization needs to contact persons within a certain geographic area, contact details and addresses may be shared, age and gender may not.
v. What are the objectives of the data sharing? Is the purpose of the data requester in line with the purpose for which the data was collected?

[3] S.S.4,7,14 The Prevention of Electronic Crimes Act 2016

vi. Could the objectives be achieved without sharing the Personal Data or anonymising it?
vii. What are the risks associated with the data sharing? Would any individual be likely to object or be harmed by the sharing? Might the sharing damage the reputation of the Organization if made public?
viii. Is the sharing reasonable and likely to be expected by the persons whose data is being shared? If not this is a serious warning bell against data sharing.
ix. When should it be shared? Is it systemic sharing, or only upon the occurrence of certain events.
x. Who else will the data be shared with? Consider including restrictions on onwards sharing in the written agreement. This may be particularly important if overseas sharing is envisaged.
xi. Are the data sharing systems compatible? Will the sharing result in corruption, loss or degradation of the data?

14.2 Sharing Personal Data with Private Entities

Where an Organization decides to share Personal Data with a private entity, it must enter into a legally binding contract prior to sharing such Personal Data. This contract must include clauses regarding data security of an equivalent or higher standard to those set out at Annex F. The terms of such clauses should be reviewed and updated regularly. Where Organizations have already started sharing Personal Data with private entities, they should consider asking the private entities to sign an addendum to the contract which includes the clause at Annex F. This may be particularly important if the Organization is sharing Protected Personal Data, Sensitive Personal Data or highly confidential data.

14.3 Sharing Personal Data with other Organizations

Personal Data sharing broadly falls into two different categories:

- systematic, routine data sharing where the same data sets are shared between the same Organizations for an established purpose; and
- one-off decisions to share Personal Data for any of a range of purposes.

Further, Personal Data may be shared between two Data Controllers, or between a Data Controller and a Data Processor.

Where the Personal Data is being shared between Controller and Processor, a written agreement between the parties should be executed prior to the data sharing (this could use the template at Annex A, including clause 1.6). This agreement shall provide that the processor:

- processes the data only in line with the controllers' instructions; and
- has data security measures in place equivalent to or better than those of the controller.

These Protocols, and any other policy setting out the Organization's data security procedures, should be included as an annex to the agreement.

Where the sharing is between two Controllers, and:

- it is systemic, data controllers should enter into a written agreement (either an MOU or a contract) setting out the information set out at Annex A, or using the model clause;
- it is a one-off, the Organizations should consider whether a written agreement is appropriate, and in any case should document the decision in writing by using the template set out at Annexes B and C.

When Organizations request another Organization to share Personal Data, they should provide the information set out in the template 'data sharing request' form at Annex B.

14.4 Security for transfers of Personal Data

Personal Data and Confidential Data should, where possible, be encrypted for transfer, particularly if it constitutes Protected or Sensitive Personal Data. Where encryption is not appropriate, the security of the data should be protected before, during and after transfer.

Use of Portable Devices for data transfer should be phased out. Where use of Portable Devices continues, these should be password protected in accordance with Paragraph 12.6.

When transferring Protected or Sensitive Personal Data, a member of the Organization's staff should deliver it to the intended recipient, who should sign upon receipt. Where this is not possible, registered or otherwise certifiable forms of delivery should be used.

Where Personal or Confidential Data is password protected, the password should be sent separately to the data itself.

14.5 Accuracy of Shared Personal Data

Prior to sharing data the sharing Organization should take steps to ensure the accuracy of the Personal Data. The larger the data set being shared, the more steps should be taken to ensure accuracy.

Organizations should ensure procedures are in place for correcting inaccuracies in Personal Data where they are detected so that the Personal Data held by all Organizations are updated.

14.6 Managing Shared Personal Data

An employee at each of the Organizations sharing the Personal Data should be nominated as responsible for monitoring the data sharing and, where relevant, compliance with the data sharing agreement. Organizations should have procedures to react quickly to any breaches of the Agreement (see clause 18 '*Breach Management*' of these Protocols).

Organizations should review data sharing arrangements regularly, and at least annually to check whether:

i. the data sharing is still necessary for the specified objectives;
ii. the quality of the shared data remains appropriate; and

iii. retention periods and other provisions of the data sharing agreements are being complied with.

15. Accuracy

Organizations should take steps to ensure that the Personal Data they hold is accurate, throughout the period they process it. In particular, Organizations should take reasonable steps to ensure that the Personal Data they hold is complete, accurate and not misleading before starting to use the information.

Organizations should establish procedures by which individuals can contact the Organization to notify them of a change in their personal data. Organizations can do this by including the following clause in their privacy notice (template at Annex D):

Please ensure that you provide us with accurate information. Please tell us as soon as possible if there are any changes to the information we have collected about you, such as a new address, by [email address].

However, Organizations should only include this in the privacy policy where they are able to process and comply with requests to amend data. Organizations are under an obligation to correct the relevant Personal Data upon receipt of a request by an individual which is in writing, confirms the identity of the individual and stipulates the reason the information is inaccurate.

16. Review and Retention

Personal Data should not be held longer than necessary. There is no set time period which can be applied across all circumstances, instead Organizations should ensure that they regularly review the Personal Data they hold and delete it when it is no longer required for the purpose it was collected for.

Holding Personal Data beyond its useful life increases the risk of data breaches and leaks, and increases the administrative burden on Organizations posed by information access requests under The Punjab Transparency and Right to Information Act 2013 ("PTRI Act").

17. Disposing of Data

All Organizations should have procedures in place to govern the disposal of materials (either in paper or electronic form) which contain Personal Data. Where Organizations contract an external party to dispose of files containing Personal Data, they must contractually agree to dispose of the files in a manner which complies with the Organizations data protection procedures and protects the confidentiality of the Personal Data. Where Organizations are disposing of paper files containing Personal Data, shredding is the best method for ensuring the adequate destruction of the Personal Data.

18. Breach Management

18.1 What is a Breach and Why Does it Happen

A 'breach' refers to any incident which means that Confidential Data held by the Organization has been accessed in an unauthorized manner. This typically includes the loss or theft of equipment on which the data is stored, inappropriate access controls, human error, or a hacking attack but may also be caused by force majeure events.

18.2 Processes for Reporting a Breach

Organizations' breach management plan should include the following steps:

i. Identification of Breach
ii. Assessment of Breach Severity and Breach Categorization (Severe, Medium, Low)
iii. Containment and Recovery
iv. Risk Assessment
v. Notification of Breach
vi. Evaluation and Response

Identification of Breach

Organizations should ensure that all staff know who to report a breach to, and the correct method of reporting (a report should always be recorded in writing, even if it is also communicated verbally). The following information should be recorded for each breach:

i. Date and time of the breach;
ii. Date and time of detection of the breach;
iii. Name and role of person who reported the breach, and to whom the breach was reported;
iv. Description of the breach (including details of Personal Data compromised);
v. Corroborating material (e.g. error messages); and
vi. Details regarding any ICT systems involved.

Containment and Recovery

Organizations should identify who will be responsible for containing the breach, this is likely to include persons with IT experience who can isolate compromised elements of the network, where appropriate disconnect them from the network, and identify the breached security procedures or change access codes.

Risk Assessment

If a breach occurs, Organizations should analyses how severe the breach is by considering the potential adverse impacts on individuals (i.e. how likely such impacts are to materialize, and the severity of the impact if they did materialize).

Organizations should record (i) the type of data involved; (ii) the number of individuals whose Personal Data is affected by the breach; (iii) whether the leaked Confidential Data is encrypted or secured in any other way.

Notification

In some cases it may be appropriate to notify the individuals whose Personal Data has been compromised. Organizations should have processes in place for such notifications were such a need to arise and should inform individuals of (i) where to obtain further information or submit queries (email, telephone number etc.); (ii) any steps they can take to protect themselves; and (iii) how the Organization can help them in protecting themselves.

Evaluation

Following any breach Organizations should review their data security processes to identify how the breach occurred and ensure steps are taken to address the compromised system or individual.

19. Assessing Data Risk in Project Design

While designing a project, it is key to ensure that the project complies with the principles of good data governance set out in these Protocols. It is good practice to carry out a data risk screening – the steps for conducting such a screening are set out at Annex G. Organizations are encouraged to complete the steps at Annex G prior to finalizing the design of any new project. This embeds privacy and data governance concerns into project design, mitigating possible risks and data breaches at a later stage.

20. Statistical and Research Functions: Anonymising Personal Data

Many Organizations will analyse large volumes of Personal Data for research and statistical functions. In most cases it is best practice to anonymise the Personal Data held for these purposes. This helps minimize the risks of processing and sharing the Personal Data. Organizations should consider whether anonymised data is sufficient at collection, processing and sharing stages.

21. Information Requests under The Punjab Transparency and Right to Information Act 2013

Organizations are compelled to respond to requests for information from individuals under The PTRI Act. Organizations should ensure they have processes in place for handling and complying with such requests. More information about Organizations' obligations under the PTRI Act, and the application procedures followed by individuals, can be found at the Punjab Information Commission's website (https://rti.punjab.gov.pk/overview).

Annex A
Data Sharing Clause

All Data Sharing Agreements should, at a minimum, contain the following information:

1. The Personal Data to be shared;
2. Whether any of the Personal Data constitutes Protected or Sensitive Personal Data;
3. The purpose, or purposes, of the sharing;
4. How the sharing is in line with the Organization's statutory (or in limited circumstances, PC-1) functions (specific element of statute should be quoted)
5. Named contacts in each Organization responsible for the Personal Data
6. The frequency of the proposed data sharing (e.g. does it constitute a pooling of data systems, is it only upon the occurrence of specified events)
7. The method of transferring data (e.g. secure email, shared access to networks)
8. Data quality – accuracy, relevance, usability etc.;
9. Confirmation by the requesting entity that the Personal Data will be processed in line with the sharing Organization's data handling protocols and security measures;
10. Clauses setting out the minimum data security measures to be complied with;
11. A statement that the receiving party will take responsibility for protecting the data upon confirmed receipt of the data;
12. Procedure for identifying and notifying breaches (i) in the transfer of data; (ii) following completion of the transfer;
13. The length of time the Personal Data will be retained by the requesting Organization (this may be either a period of time, or linked to the achievement of certain objectives);
14. How the data will be deleted securely after expiry of the retention period;
15. Review and termination of the agreement; and
16. Sanctions for failure to comply with the agreement or breaches by individual staff.

A sample Data Sharing Clause is set out below:

DEFINITIONS

Agreed Purposes: [STATE THE PURPOSES FOR WHICH THE PERSONAL DATA IS TO BE HELD. FOR ORGANISATIONS THIS WILL TYPICALLY REQUIRE A STATEMENT AS TO THE GOVERNMENT FUNCTION THE DATA IS REQUIRED TO FULFIL – QUOTE STATUTE/RULES OF BUSINESS WHERE POSSIBLE].

Data Discloser: [NAME OF PARTY DISCLOSING DATA]

Data Protection Regulation: (i) The Prevention of Electronic Crimes Act 2016; (ii) the Data Processing Protocols at Annex [1] [DATE]; and (ii) any other applicable regulation or legislation relating to data security and usage. [Note: Append Protocols to Agreement where the agreement is between two Organizations only]

Data Receiver: [NAME OF PARTY REQUESTING & RECEIVING DATA]

Permitted Recipients: The parties to this agreement, the employees of each party, any third parties engaged to perform obligations in connection with this agreement, and [ADD ANY OTHER PERMITTED RECIPIENTS].

Shared Personal Data: the personal data to be shared between the parties under clause 1.1 of this agreement. Shared Personal Data shall be confined to the following categories of information relevant to the following categories of data subject:

a. [type of personal data];

b. [type of personal data], and

c. [type of personal data].

1. Data Protection

1.1 Shared Personal Data. This clause sets out the framework for the sharing of personal data between the parties as data controllers. The Data Sharer will regularly disclose to the Data Receiver the Shared Personal Data for the Agreed Purposes.

1.2 Data Sharing Mechanism. The Shared Data will be shared by [*Detail the method of data transfer, e.g. secured email/shared access to network etc.]*

1.3 Timing of Data Sharing. The Shared Personal Data will be shared [*upon occurrence of a specific event, e.g. upon achievement of certain project milestones, or upon signing of the Agreement, or during a certain time period*]

1.4 Effect of non-compliance with Data Protection Regulation. Each party shall comply with all the obligations imposed on a controller under the Data Protection Regulation, and any material breach of the Data Protection Regulation by one party shall, if not remedied within 30 days of written notice from the other party, give grounds to the other party to terminate this agreement with immediate effect.

1.5 Particular obligations relating to data sharing. Each party shall:

a) ensure that it its data privacy policies envisage the data sharing to the Permitted Recipients for the Agreed Purposes;

b) process the Shared Personal Data only for the Agreed Purposes;

c) Use reasonable endeavors to ensure that the Shared Personal Data is accurate, and notify the other party if it becomes aware of any inaccuracy

d) not disclose or allow access to the Shared Personal Data to anyone other than the Permitted Recipients;

e) ensure that all Permitted Recipients are subject to written contractual obligations concerning the Shared Personal Data (including obligations of confidentiality) which are no less onerous than those imposed by this agreement;

f) ensure that it has in place appropriate technical and organizational measures, reviewed and approved by the other party, to protect against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data, these should include, but not be limited to:

i. ensuring access to the Personal Data is limited to employees that need to process the data in order to fulfill their professional tasks;

ii. ensure access is protected by password of at least 8 characters;

iii. [the personal data is encrypted;] [*Note: Consider referring to minimum security standards, IT staff to review.*]

g) notify the other party without undue delay on becoming aware of any breach of the Data Protection Regulation or other data breach;

h) use compatible technology for the processing of Shared Personal Data to ensure that there is no lack of accuracy resulting from personal data transfers;

i) maintain complete and accurate records and information to demonstrate its compliance with this clause 1.5 [and allow for audits by the other party or the other party's designated auditor]; and

1.6 [**Instructions for Processing**. The Data Receiver will only process the Shared Personal Data in line with the instructions of the Data Discloser] [*Note: This should only be included where the Data Receiver is acting as a processor and only handling data on the Data Discloser's instructions.*]

1.7 **Retention.** The parties shall only retain the Shared Personal Data for [*set period of time / the duration of the Agreement / as long as is necessary for fulfilling the Agreed Purpose*]

1.8 **Data Sharing Manager**. The Data Discloser nominates the following employee as point of contact and responsible manager for all issues arising out of the Data Sharing:

Name:
Title:
Email:
Telephone:

The Data Receiver nominates the following employee as point of contact and responsible manager for all issues arising out of the Data Sharing:

Name:
Title:
Email:
Telephone:

1.9 **Deletion.** The Data Receiver shall at the written direction of the Data Discloser, delete or return Shared Personal Data and copies thereof to the Data Discloser on termination of this agreement unless required by law to store the personal data.

Annex B

Personal Data Sharing Request Form

Name of Organization requesting sharing of Personal Data:	
Name(s) of Organization (s) request sent to:	
Date of request:	
Date Personal Data required by:	
Personal Data being requested:	
(i) By type	
(ii) By number of individuals data relates to (rounded to nearest 10)	
Purpose Personal Data will be used for:	
Name of person requesting Personal Data:	
Title of person requesting Personal Data:	
Please specify if data is to be shared with other organizations (and if so list them)	
Is the request in line with an existing data sharing agreement?	
Is a new data sharing agreement contemplated?	
Signed:	

Annex C

Data Sharing Decision Form

Name of Organization receiving data sharing request:	
Name of Organization requesting Personal Data:	
Date of Request:	
Date request received:	
Date response requested:	
Personal data being requested:	
(iii) By type	
(iv) By number of individuals data relates to (rounded to nearest 10)	
Purpose of data request:	
Reason(s) for disclosure or non-non-disclosure:	
Is sharing with named organizations permitted? *Note: Any sharing not explicitly authorized is prohibited and the requesting Organization shall be held responsible for any data breach.*	
Is the data sharing covered by a data sharing agreement? (if yes specify date of execution)	
Date of disclosure/rejection of request:	
Decision taken by (name and position):	
Signed:	

Annex D
Template Privacy Policy

The [*Organization Name*] collects certain elements of information about you in order to comply with applicable laws and regulations and carry out [*Organization Name*'s] and associated public functions. Some of this information identifies you as an individual and therefore constitutes personal data. We have policies in place to guide how we handle the personal data we hold about you. We are careful in how we collect and use your personal data and are committed to maintaining the security of your data and respecting your privacy rights.

Information Collected when you visit the Website

When you visit our website we may collect the following types of information:

- Your [*name / telephone number / address / CNIC*] if you provide feedback or suggestions to [the Organization's name]
- Details of how you use the site, using cookies and other techniques
- Your Internet Protocol (IP) address
- [*include any other information which can be gathered from the user on the website*]

This data is used by [*the Organization*] to:

- administer this website
- improve the functionality of the website
- obtain feedback on the services we provide
- contact you in response to feedback or suggestions you provide
- [*any other use of the data collected on the website*]

Cookies

Our website use cookies to collect information. Cookies are small text files that are downloaded onto your device as you browse websites. Cookies on our website collect information about your browsing behavior, uses preference and past actions. Cookies are key to the functionality of many websites, and help tailor the browsing experience to you.

Cookies on our website collect [*detail the types of information*].

You can disable cookies, so that your computer blocks them or alerts you each time they are being used, by changing your web browser settings. Exactly how to do this will depend on the browser you use – look at your browser's Help Menu to identify how to change your cookie preferences.

The website may not operate properly if cookies are switched off.

[Note: If using third party cookies state this and include a statement that 'If you only disable third party cookies you will still be able to use our website, even if the functionality is partly impaired.']

Information we collect in Performing Public Functions

We may collect other information about you in order to perform our own and associated public functions effectively and efficiently. These include:

[*Please set out the relevant government functions data is required for, e.g. for law enforcement authorities this would likely include, 'investigating an offence, detecting, preventing or prosecuting a crime'. In all cases you can include 'delivering public services; verifying your identity to provide services; contacting you.*]

Sharing the information you provide to us

We may share the information we hold about you if we are required to do so by law. We may also share the information with other government departments or bodies for the fulfillment of their functions. This may include police and law enforcement authorities, the courts, and foreign law enforcement bodies or government authorities.

[*If the Organization share personal data with private parties, include the following: 'In some instances we share information with private parties who process information [on our instructions] in order to [e.g. deliver services on our behalf].' Consider in what instances sharing with private parties will be appropriate. It is likely to be only where the private party acts as processor, i.e. processes the personal data on the instructions of the Organization. If this is the case, state this.*]

[*If the Organization does not share personal data with private parties, include the following: We will not share the information you provide to us with other websites [, private entities,] or for marketing purposes.*] [*Organizations to verify this and tailor accordingly]*

We will not share the information we hold about you for commercial uses.

How long we hold your information for

We will hold the data for as long as needed to provide you with the relevant service or conduct the relevant [Organization name] or associated functions. We may hold your data for longer where regulations require us to do so.

The security of your data

Transferring data over the internet is typically not entirely secure - we cannot guarantee the safety of your data when it is being transferred to us.

Once we receive your data, we have procedures and protocols in place to keep your data secure and avoid any unauthorized access to your data.

Links to other website

Where you click a link on our website which takes you to a different website, our Privacy Notice no longer applies.

Annex E
Model Data Protection Clause for Inclusion in Employment Contracts

[*Note: The Protocols should be attached as an annex to the employment contract. Square brackets indicate where the Organization should tailor the clause.*]

1. [The Organization] shall collect and process information relating to the Employee in order to fulfill human resource and payroll functions and other functions.

2. The Employee shall comply with the Data Processing Protocols when handling Confidential Data in the course of employment including personal data relating to any employee, customer, client, supplier or agent of the Company. The Employee will also comply with the Organization's [ANY OTHER RELEVANT POLICY E.G. IT].

3. The Employee shall not share any Confidential Data obtained in the course of their employment with the Organization without appropriate permission from the Organization.

4. Upon termination of the Employees' employment with [the Organization], due to the expiry of this Contract or for any other reason, the Employee shall either destroy or return to [the Organization] all Confidential Data, according to [the Organization's] instructions.

5. Failure to comply with this clause, the Data Processing Protocols [or any of the policies listed above in Clause [●]] may be dealt with under [Organization Name] disciplinary procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

Definitions:

Confidential Data: all data shared by the Organization with the Employee which is either Personal Data or is not in the public domain.

Personal Data: information which, either on its own or in combination with other information the Employee holds, can be used to identify an individual.

[Data Processing Protocols: the document attached at Annex [●]. *Note: definition only accurate if appropriate to annex protocols.*]

Annex F
Model Data Sharing Clause for Private Parties

Note: Square brackets indicate where this clause should be tailored to the specific circumstances of the agreement. Organizations must include this clause with reference to 'Organization Personal Data.' In some circumstances Organizations may wish to bind the Service Provider to the conditions set out below in relation to all data shared with them. In these cases, use the defined term 'Organization Data'.

1) The Service Provider shall:
   a) Ensure it has in place appropriate technical and organizational measures to protect against unauthorized or unlawful processing of [Organization Data / Organization Personal Data] and against accidental loss or destruction of, or damage to, [Organization Data / Organization Personal Data];
   [*Note: If minimum security criteria have been agreed, detail them here/refer to an annex where they are set out. Consider taking the security provisions of the Protocols and referring to these as minimum provisions.*]
   b) [Process [Organization Data / Organization Personal Data] only in accordance with the Organization's instructions;] [*Note: This should only be included where the private entity is acting as a processor and only handling data on the Organization's instructions.*]
   c) Process the [Organization Data / Organization Personal Data] only for the Agreed Purposes;
   d) Notify the Organization within one (1) Business Day of any data breach which might have compromised [Organization Data / Organization Personal Data];
   e) Securely destroy or return any or all [Organization Data / Organization Personal Data] (i) when requested to do so by the Organization; or (ii) upon termination of the Contract;
   f) Not disclose or permit access to the [Organization Data / Organization Personal Data] to anyone other than the Permitted Recipients; and
   g) ensure that all Permitted Recipients are subject to written contractual obligations concerning the [Organization Data / Organization Personal Data] (including obligations of confidentiality) which are no less onerous than those imposed by this agreement.

Definitions

Organization Data: all data shared by the Organization with the Service Provider.

Organization Personal Data: data shared by the Organization with the Service provider which, either on its own or in combination with other information the Service Provider holds, can be used to identify an individual.

Agreed Purposes: [*Detail the purposes for which you have agreed the data will be shared. These should be specific and limited.*]

Permitted Recipients: [*Set out the names of organizations the Service Provider may share data with, if any.*]

Annex G

Screening Projects for Data Risk

All projects should be screened at the design phase to identify if they pose a risk to the privacy of individuals or the data governance of Organisations. If such risks identified, and they will exist in a significant proportion of projects, particularly in the social sectors, they should be addressed by the three step procedure below. Ensure that internal, and where relevant, external, consultation is conducted with all relevant parties, this may include IT officers to enhance data security provisions and third parties who will be involved in processing the data.

STEP 1: SCREENING

The first step is to decide whether there exists a persona data / privacy risk – if the answer to any of the questions set out below is yes, then a risk exists and steps 2 to 4 should be completed. If the answer to all the questions below is no, and it is believed no data risk exists, there is no need to complete steps 2 to 4, however the conclusions of this Step 1 should be recorded, with reasons, to be referred to in the future if necessary.

- In order to execute the project will you be collecting new information about individuals?
- Does the project involve sharing personal data with Organisations or persons who have not previously had access to it?
- Does the project propose using personal data already held by the Organisation for a new and different purpose to that for which it is currently used?
- Does the project involve the digitisation of paper records which include personal data?
- Does the project involve consolidating existing data sets, which include personal data, into new systems or databases?
- Will the project require contact with individuals? Is this contact likely to be perceived as intrusive?
- Does the project use information about individuals which is likely to be considered sensitive e.g. criminal or health data?
- Does the project involve using new technology which utilize personal data e.g. surveillance cameras or biometric technologies?

STEP 2: MAPPING INFORMATION FLOWS

In order to fully understand the data risks presented by the project, it is necessary to map out the flows of data the project requires.

- What personal data is required?
- How is the information going to be obtained, used, stored and deleted? (consider data security, retention periods, deletion methods)
- Is all the information necessary for the project?
- What purposes are the personal data needed for?
- Who will have access to the personal data?
- Will the personal data be shared with other Organisations or the private sector?

STEP 3: IDENTIFY RISKS

Try and identify where there are risks that the information collected may be shared further, or used for a purpose other than that original envisaged.

- Is it likely the information collected may be shared with other Organisations or the private sector?
- Is it likely that the personal data may be used for a purpose other than that originally envisaged?
- Is the data particularly sensitive or confidential?
- Is the scope or type of data collection proposed proportionate to the objectives of the project? Consider whether it may be seen as overly intrusive by individuals?
- Would the data cause reputational harm either to Government or to the relevant individual if leaked/breached?
- Are retention periods set? If not, this constitutes a risk.
- Is the relevant Organisation able to respond to any requests for information under the Right to Information and Transparency Act?

STEP 4: INTEGRATING SOLUTIONS IN PROJECT DESIGN

Once a solution is identified it should be integrated back into the project planning so that the final project structure presents the lowest data risk possible.

- Can the data be anonymised?
- Can the project operate with less personal data than originally envisaged?
- Can you put in place contractual safeguards to protect data being shared? E.g. by ensuring that written contracts with data protection clauses are entered into between parties prior to sharing the data (See Section 14 of the Data Processing Protocols).
- Can you enhance the security measures in place to protect the data?
- Can you amend your privacy notice to be more transparent about the data processing envisaged under the project?
- Can you put in place mechanisms to ensure the data collected remains accurate?
- Can you provide training to relevant staff to mitigate risk of data leaks / unauthorized use?