

# DATA & PRIVACY PROTECTION PROCEDURES (DP3)



# PSCA

Punjab Safe Cities Authority

PPIC3 CENTER

📍 Qurban Lines, Lahore

☎ 042 99 05 16 05

🌐 [www.pzca.gov.pk](http://www.pzca.gov.pk)

✉ [info@pzca.gov.pk](mailto:info@pzca.gov.pk)



## **BACKGROUND:**

The protection of natural person in relating to the processing of personal data is a fundamental right, which is enshrined in the Article 14 (1) of the Constitution of Pakistan Islamic Republic of Pakistan 1973<sup>1</sup>. It is, therefore, necessary for security institutions like Punjab Safe Cities Authority to have a well-defined Data and Privacy Protection Procedures (DP3) which have detailed guidelines for users and recipients of PSCA data. It becomes more critical because it has repercussions for multiple stakeholders involved in the process.

Punjab Safe Cities Authority has to meet requirements of law enforcement agencies as well as protecting the data being generated, gathered or stored and shared with lawful authorities not only for safety and security while duly protecting the rights of the persons who are involved and subjects of this data. In this age of digitalization, personal data of any person can easily be misused, modified and shared for criminal or other malicious purposes. Data should be secured according to the designated parameters and not shared internally or externally without prior approval of courts or competent authority with a due process. These DP3 are subjected to changes implemented from time to time and made available to all publicly.



## **1. INTRODUCTION:**

In 2016, through a consultative process, PSCA requested the Federal Government of Pakistan, through Government of the Punjab, to address the issue of admissibility of the evidence collected through electronic device in all cases of criminal law. Following this, as a Part of Punjab Police, it has a constitutional obligation to protect the citizens of Pakistan and in Punjab, therefore, PSCA has introduced for the first time in Pakistan, Data Protection and Privacy Procedures (DP3) with guidelines since 2016. Subsequently These were implemented to harmonies the protection of fundamental rights and freedom of the natural person in respect of processing data generated and maintained by PSCA, that is in line with the following legal instruments:

<sup>1</sup> Part II, Fundamental Rights and Principles of Policies, Constitution of Islamic Republic of Pakistan, 1973

- |   |   |
|---|---|
| <p><b>1</b> Article 14(1) of The Constitution of the Islamic Republic of Pakistan 1973 <sup>2</sup></p> | <p><b>2</b> The Prevention of Electronic Crimes Act (PECA) 2016 <sup>3</sup></p>                  |
| <p><b>3</b> Convention on the Rights of the Child <sup>4</sup></p>                                      | <p><b>4</b> International Covenant on Civil and Political Rights (ICCPR) <sup>5</sup></p>         |
| <p><b>5</b> Pakistan Penal Code 1860 <sup>6</sup></p>   | <p><b>6</b> General Data Protection Regulation (GDPR) 2016/679 of European Union <sup>7</sup></p> |
| <p><b>7</b> PSCA Electronic Data Regulations 2016 <sup>8</sup></p>                                      | <p><b>8</b> Cairo Declaration on Human Rights in Islam 1990 (CDHRI) <sup>9</sup></p>              |
| <p><b>9</b> The Investigation of Fair Trial 2013 <sup>10</sup></p>                                      | <p><b>10</b> Any other relevant framework applicable from time to time</p>                        |

<sup>2</sup> The Article deals with the dignity of man and, the privacy of home subject to law, shall be inviolable.

<sup>3</sup> PECA 2016 is promulgated to prevent unauthorized acts such as electronic forgery & fraud, cybercrime, hate speech, child pornography, spamming, spoofing and provide mechanism for their investigation, prosecution and trial.

<sup>4</sup> To recognize the special care and assistance to the child because of his physical & mental immaturity and to grownup in a family environmental, atmosphere of happiness, love and to live an independent life including appropriate legal protection before as well as after birth

<sup>5</sup> Defines & includes the inherent dignity of human person, the idea of free human being to enjoying civil & political freedom and to safeguard his economic, social and cultural rights.

<sup>6</sup> Section 509, of Pakistan Penal Code defines insulting modesty or causing harassment, section 499 of PPC define defamation, section 268 of PPC ie that is public nuisance and section 409 of PPC defines Criminal breach of trust by public servant, or by banker, merchant or agent and in case of approve the guilt punishment for life & fine may be awarded to the culprits.

<sup>7</sup> Free data within European Union not restricted nor prohibited for reason to connect with the protection of natural persons with regard to the processing of personal data

<sup>8</sup> PSCA since its inception is mindful of the privacy concerns and has adopted a process how to collect evidence/data from PPIC3/PSCA and to whom this data/evidence may be provided for investigation, enquiry and trial keeping in mind present requirements, human rights framework and international obligations of the state from Privacy perspective. PSCA also recommended in 2018 to expand the scope of concept of Privacy from home to public places as well.

<sup>9</sup> CDHRI reaffirms that all human beings are from one family without any discrimination on the ground of race, color, language, sex, religious belief and the life is God-given gifted. The struggle to protect a person from exploitation, prosecution, and to affirm his freedom and right to a dignified life witch are contained in the Revealed Books of Allah should be thorough

<sup>10</sup> Investigation for collection of evidence by means of modern techniques and devices to prevent and effectively deal with scheduled offences and prohibition of misuse of interception material.

## **2. OBJECTIVES:**

---

These DP3 and guidelines, primarily, are conceived and implemented:

- I.** To protect Privacy rights of the people through PSCA systems;
- II.** To secure the data of natural person and events collected and maintained by PSCA for security and public safety purposes;
- III.** To maintain the integrity of the Evidence/data being delivered to honorable Court/Forum or on their direction to any person and to Law Enforcement Agencies (LEA) through PSCA infrastructure;
- IV.** To retain, preserve, store and destroy the electronic data gathered/collected through electronic devices of PPIC3/PSCA and its provision protocols to Law Enforcement Agencies/Courts/Tribunals / Investigating officers etc.;
- V.** To retain, preserve, store and destroy the electronic data gathered/collected through electronic devices of PPIC3/PSCA and its provision protocols to Law Enforcement Agencies/Courts/Tribunals / Investigating officers etc.;



## **3. INSTALLATION OF SURVEILLANCE NETWORK/SENSORS BY PSCA:**

---

- I.** PSCA cameras and sensors will not be installed in any place which may affect the protection of Privacy rights of the people in public or private without due process and authorization.
- II.** PSCA cameras and sensors shall only be placed at public places or any other place directed by the Government/Authority.
- III.** PSCA cameras and sensors shall be placed at conspicuous places so people can observe and remain informed about the presence of such equipment.
- IV.** Presence of cameras and sensors in Punjab shall be publicly shared in order to maintain deterrence and privacy rights of public to the best possible extent without compromising requirement of the law enforcement agencies and PSCA.
- V.** Data obtained through any cameras and sensors and equipment shall be used only as per the guidelines of the Authority including the instructions contained in this policy and procedures.



## 4. PSCA'S DATA USERS GUIDELINES:

---



- I.** Only authorized persons and entities can access, view, listen, use, alter, copy, transfer, publish and/or obtain data from PSCA through a lawful process.
- II.** Stored/gathered data shall be shared with only authorized person internally or externally.
- III.** Investigation Officers or representative of any security agency can only access, listen or view data of an incident by visiting PSCA with prior approval and after following due process.
- IV.** No data from PSCA shall be shared without watermarks and clear identification for tracking back the data and the process.
- V.** No Officer/user at PSCA shall be allowed to store any data in any unauthorized manner or unauthorized purpose.
- VI.** No data shall be shared with any LEA or Court in such arrangement, which may lead to further use or disseminate easily.
- VII.** An approved Electronic Data Analysis procedure shall be followed for sharing any data to any LEA or Court.
- VIII.** Data shall not be managed or handled by any person who is not provided sufficient training and have requisite knowledge about the Standing Operating Procedures and lawful requirement about Electronic Data Regulations.
- IX.** Data including live feed shall not be shared with any other organization without lawful permission and processes in order to secure the fundamental privacy rights of citizens and for sanctity of evidential value of the data.
- X.** A person who is reasonably found to misuse his/her rights and authorizations of data handling, protection, transfer or custodian of any data shall be liable for any civil and/or criminal consequences as per law by the Authority.

## 5: Data Handling Procedure:

- I. All users of PSCA data, whether collected through PSCA infrastructure or disseminated through the systems, including social and electronic media, shall adhere to DP3.
- II. PSCA/PPIC3 Officers/officials or any other authorized/allowed person (Officers) shall not deliberately record any act of natural person at a public place or inside any vehicle infringing their right of privacy unless there is reasonable reason to believe that they are committing or attempt to committing any offence.
- III. Officers shall remain very careful while gathering any data of Women and Children.
- IV. Officers shall not use or store any data in their personal devices otherwise in accordance with the directions of competent authority.
- V. Officers shall not monitor any personal space of citizen unless necessary and proportionate to their lawful requirements.
- VI. Officers shall not disseminate/publicize any objectionable pictures/videos of persons in any form through any medium which may infringe upon the rights of persons involved in the pictures/videos.
- VII. Track record of accessing data is maintained by all the employees of PPIC3/PSCA deputed as operators.
- VIII. Any violation of DP3 will be considered as misconduct, as per Service Regulations 2017 of PSCA and disciplinary action shall be taken against any officer/employee found violating these obligations.
- IX. Without prejudice to any other civil or criminal legal consequence, contract of operators may be terminated due to violations of DP3.



## 6: Data Sharing Terms & Conditions:

- I. This Electronic Data Application Form is available free of cost and can be accessed and downloaded from Authority's official website [www.pzca.gov.pk](http://www.pzca.gov.pk).
- II. A request for electronic evidence is made for the purposes of, providing evidence in criminal, civil, family or any Court/Tribunal proceedings, prevention & reduction of crime & disorder, investigation and detection of crime, identification of witnesses and other lawful purposes.



- III.** The Applicant shall apply for the delivery of electronic data based on reliable/trustworthy details as mentioned in the application form.
- IV.** The details given in the application form by the applicant should be correct, accurate and best to the knowledge of the applicant in its official capacity.
- V.** The applicant shall be liable for any misstatement, false data or concealment, for obtaining electronic data.
- VI.** The applicant shall affirm that he/she has requested for electronic data in official capacity and for lawful purpose.
- VII.** The electronic data should only be used for the purpose and scope mentioned in the application form, and received data could not be used for any other purpose.
- VIII.** The Applicant shall be responsible for any damage/loss/tempering to the electronic data/Electronic Data Storage Device after receiving evidence in electronic form i.e. USB Storage/other medium.
- IX.** The Applicant shall take all necessary measures for protection of data/electronic evidence and to submit in the court as a primary evidence.
- X.** The Applicant shall only be able to view the content of the Electronic Data in the premises of IC3 center after due process before its delivery to the Applicant.
- XI.** It shall be the responsibility of the Applicant to store in safe custody the received Electronic Data Storage Device in its original form and its further transmission to the court for further legal procedure.
- XII.** The Applicant shall be liable for any tempering/edition/deletion of the content after its delivery to the Applicant.
- XIII.** The Electronic Data shall be an admissible piece of evidence in the court of law/competent forum and is governed by the provisions of PSCA Electronic Data Regulations 2016 along with other enabling provisions of applicable law(s).
- XIV.** The Applicant shall ensure security of Electronic Data Storage Device, USB storage/other medium issued to the applicant and follow every procedural, security and other requirement as specified by the authority.
- XV.** The Authority may charge a fee on issuance of Electronic Data and the USB Storage/Other medium and other related equipment and services.
- XVI.** The Authority shall provide expert assistance to the applicant and to the Court in regards to the technical matters related to the Electronic Data.
- XVII.** The Video/Audio/Image/Electronic Data shall be provided in its original form.
- XVIII.** The content shall be given in original form. The content contained in the USB Storage/Other Medium shall be the true form of the original Video/Audio/Image stored on the main data center of IC3 center(s) after due watermarking.
- XIX.** The Electronic Data shall be saved for 30 days after it is stored/transmitted/provided/sent/made available in Electronic Data Storage and delivered/handed



over to the investigation officer or presented to the court.

**XX.** Electronic Evidence already stored/preserved may be saved up-to 7 years, if the Authority is satisfied that the information/video/audio/sound/pictures are required to be stored till such time,

**XXI.** The applicant shall officially inform about the final decision of the court/tri-bunal/competent authority in regards the abovementioned incident in which the data/evidence delivered to him. In case the data is no more required, it shall be deleted from the storage of IC3 center.

**XXII.** The Application can only be made within 30 days of the incident/occurrence or as specified by any court of law.

**XXIII.** Copyright and ownership of all material recorded by virtue of the electronic system shall remain with the Authority and IC3 data center.

**XXIV.** Authority can be contacted at support.evidence@psca.gop.pk for further assistance or related information.

**Note:**

These DP3 guidelines are issued to ensure that lawful operations of safety and security by PSCA officer, men and women, are executed keeping in mind the fundamental Human rights regime of the country without compromising security and privacy perspectives.

Notwithstanding the forgoing, PSCA reserves the right to revise, revoke, or amend this policy from time to time.

**Join us for Data & Privacy Protection:**

If you have any suggestions or you notice any violation of DP3, please inform us through email Privacy.Protection@psca.gop.pk or call 15 for complaint.



**PPIC3 CENTER**

Qurban Lines, Lahore Pakistan



[www.pasca.gop.pk](http://www.pasca.gop.pk)



042 990 456 05



[info@psca.gop.pk](mailto:info@psca.gop.pk)



@punjabsafecities



@PSCAsafecities