Policy 2018 Online

Digital Security Act

Bangladesh

Data Governance

Definitions of Data:

Main Focus of Document:

To ensure national digital security and to enact laws pertaining to digital crime identification, prevention and suppression.

Target Beneficiaries or Sectors:

N/A

Key Elements:

There is provision for a digital forensic lab to be created for the analysis of digital matters; along with a digital forensic agency which will oversee all digital matters and a computer emergency response team that will be responsible for cyber attacks and ensure that critical information remains secure. Key details include: 27) Punishment for committing cyber-terrorism: (1) If any person –

a. With the intention to breach the national security or to endanger the sovereignty of the Nation and to instill terror within the public or a part of them creates obstruction in the authorized access to any computer, computer network or internet network or illegally accesses the said computer, computer network or internet network or cause the act of obstruction of access or illegal entry through someone, or
b. Creates such pollution within any digital device or inserts malware which causes the death of a person or results in serious injury to a person or raises a possibility of it, or
c. Damages or destroys the supply of daily necessities of public or adversely affects any critical information infrastructure
d. Intentionally or knowingly enters or penetrates any computer, computer network, internet network, any secured data information or computer database or such secured data information or computer database which can be used to damage friendly relations with another foreign country or can be used for acts against public order or which can be used for the benefit any foreign country or any foreign person or any group. Then that activity of that person will be considered as cyber security crime. (2) If any person commits any offense mentioned within sub section (1), the person will be penalized with imprisonment for a term not exceeding 14 years or with a fine not exceeding 1 crore taka or with both. (3) If any person commits the offense mentioned in sub-section (1) for the second time or recurrently commits it then, he will be punished with lifetime imprisonment or with fine not exceeding 5 crore taka or with both.

33. Illegal transferring or saving of data or information, and resulting punishment: (1) If any person enters any computer or digital system illegally and does any addition or subtraction, transfer or with the aim of transfer save or aid in saving any data or information belonging to government, semi-government, autonomous or statutory organization or any financial or commercial organisation , then the activity of that person will be considered an offence. (2) If any person commits an offence mentioned in sub-section (1), he will be sentenced to a term of imprisonment not exceeding 5 years or with fine not exceeding Tk.10 lac or with both. (3) If any person commits the offence mentioned in sub-section (1) a second time or recurrently commits it, then he will be sentenced to a term of imprisonment not exceeding 7 years or with fine not exceeding Tk.15 lac or with both.

34. Data preservation:

35. If the Director General on his own accord, or on the basis of an application by the investigation officer, believes that any data or information stored in a computer should be preserved for the interest of an investigation under this Act or there is possibility that such information could be harmed, destroyed, altered or lost, then he/she can order the person or institution responsible for that computer or computer system to preserve such data or information for 90 days. (2) Tribunal may, on application, extend the period of preservation of such data or information, but it should not be for more than a total of 180 days.

Data Data preservation Digital infrastructure Internet

Policy/regulation mirrored:

Countries: