[IRR OF REPUBLIC ACT NO. 10173, August 24, 2016]

IMPLEMENTING RULES AND REGULATIONS OF REPUBLIC ACT NO. 10173, KNOWN AS THE "DATA PRIVACY ACT OF 2012"

Pursuant to the mandate of the National Privacy Commission to administer and implement the provisions of the Data Privacy Act of 2012, and to monitor and ensure compliance of the country with international standards set for data protection, the following rules and regulations are hereby promulgated to effectively implement the provisions of the Act:

Rule I. Preliminary Provisions

1. Title
2. Policy
3. Definitions

Rule II. Scope of Application

4. Scope
5. Special Cases
6. Protection afforded to data subjects
7. Protection afforded to journalists and their sources

Rule III. National Privacy Commission

8. Mandate
9. Functions
10. Administrative Issuances
11. Reports and Public Information
12. Confidentiality of Personal Data
13. Organizational Structure
14. Secretariat
15. Effect of Lawful Performance of Duty
16. Magna Carta for Science and Technology Personnel

Rule IV. Data Privacy Principles

17. General Principles
18. Principles of Transparency, Legitimate Purpose and Proportionality
19. Principles in Collection, Processing and Retention
    a. Collection must be for a specified and legitimate purpose
    b. Personal Data shall be processed fairly and lawfully
    c. Processing should ensure data quality
    d. Personal data shall not be retained longer than necessary
    e. Any authorized further processing shall have adequate safeguards
20. Principles for Data Sharing

Rule V. Lawful Processing of Personal Data

21. Lawful Processing of Personal Information
22. Lawful Processing of Sensitive Personal Information and Privileged

Information
23. Extension of Privileged Communication
24. Surveillance of Subjects and Interception of Recording of Communications

Rule VI. Security Measures for Protection of Personal Data

25. Data Privacy and Security
26. Organizational Security
27. Physical Security
28. Technical Security
29. Appropriate Level of Security

Rule VII. Security of Sensitive Personal Information in Government

30. Responsibility of Heads of Agencies
31. Requirements Relating to Access by Agency Personnel to Sensitive Personal Information
32. Implementation of Security Requirements
33. Applicability to Government Contractors

Rule VIII. Rights of Data Subject

34. Rights of the Data Subject
    a. Right to be informed
    b. Right to object
    c. Right to access
    d. Right to correct
    e. Right to rectification, erasure or blocking
35. Transmissibility of Rights of the Data Subject
36. Right to Data Portability
37. Limitation on Rights

Rule IX. Data Breach Notification.

38. Data Breach Notification
39. Contents of Notification
40. Delay of Notification
41. Breach Report
42. Procedure for Notification

Rule X. Outsourcing and Subcontracting Agreements.

43. Subcontract of Personal Data
44. Agreements for Outsourcing
45. Duty of Personal Information Processor

Rule XI. Registration and Compliance Requirements

46. Enforcement of the Data Privacy Act
47. Registration of Data Processing Systems
48. Notification for Automated Processing Operations
49. Review by the Commission

Rule XII. Rules on Accountability

50. Accountability for Transfer of Personal Information
51. Accountability for Violation of the Act, these Rules and other issuances

Rule XIII. Penalties

52. Unauthorized Processing of Personal Information and Sensitive Personal Information
53. Accessing Personal Information and Sensitive Personal Information Due to Negligence
54. Improper Disposal of Personal Information and Sensitive Personal

Information
55. Processing of Personal Information and Sensitive Personal Information for Unauthorized Purposes
56. Unauthorized Access or Intentional Breach
57. Concealment of Security Breaches Involving Sensitive Personal Information
58. Malicious Disclosure
59. Unauthorized Disclosure
60. Combination or Series of Acts
61. Extent of Liability
62. Large-Scale
63. Offense Committed by Public Officer
64. Restitution
65. Fines and Penalties

Rule XIV. Miscellaneous Provisions

66. Appeal
67. Period for Compliance
68. Appropriations Clause
69. Interpretation
70. Separability Clause
71. Repealing Clause
72. Effectivity Clause

Rule I. Preliminary Provisions

Section 1. ***Title.*** These rules and regulations shall be known as the "Implementing Rules and Regulations of the Data Privacy Act of 2012", or the "Rules".

Section 2. ***Policy.*** These Rules further enforce the Data Privacy Act and adopt generally accepted international principles and standards for personal data protection. They safeguard the fundamental human right of every individual to privacy while ensuring free flow of information for innovation, growth, and national development. These Rules also recognize the vital role of information and communications technology in nation-building and enforce the State's inherent obligation to ensure that personal data in information and communications systems in the government and in the private sector are secured and protected.

Section 3. ***Definitions.*** Whenever used in these Rules, the following terms shall have the respective meanings hereafter set forth:

a. "Act" refers to Republic Act No. 10173, also known as the Data Privacy Act of 2012;

b. "Commission" refers to the National Privacy Commission;

c. "Consent of the data subject" refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of his or her personal, sensitive personal, or privileged information. Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of a data subject by a lawful representative or an agent specifically authorized by the data subject to do so;

d. "Data subject" refers to an individual whose personal, sensitive personal, or privileged information is processed;

e. "Data processing systems" refers to the structure and procedure by which personal data is collected and further processed in an information and communications system or relevant filing system, including the purpose and intended output of the processing;

f. "Data sharing" is the disclosure or transfer to a third party of personal data under the custody of a personal information controller or personal information processor. In the case of the latter, such disclosure or transfer must have been upon the instructions of the personal information controller concerned. The term excludes outsourcing, or the disclosure or transfer of personal data by a personal information controller to a personal information processor;

g. "Direct marketing" refers to communication by whatever means of any advertising or marketing material which is directed to particular individuals;

h. "Filing system" refers to any set of information relating to natural or juridical persons to the extent that, although the information is not processed by equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible;

i. "Information and communications system" refers to a system for generating, sending, receiving, storing, or otherwise processing electronic data messages or electronic documents, and includes the computer system or other similar device by which data is recorded, transmitted, or stored, and any procedure related to the recording, transmission, or storage of electronic data, electronic message, or electronic document;

j. "Personal data" refers to all types of personal information;

k. "Personal data breach" refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed;

l. "Personal information" refers to any information, whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual;

m. "Personal information controller" refers to a natural or juridical person, or any other body who controls the processing of personal data, or instructs another to process personal data on its behalf. The term excludes:

    1. A natural or juridical person, or any other body, who performs such functions as instructed by another person or organization; or

2. A natural person who processes personal data in connection with his or her personal, family, or household affairs;

There is control if the natural or juridical person or any other body decides on what information is collected, or the purpose or extent of its processing;

n. "Personal information processor" refers to any natural or juridical person or any other body to whom a personal information controller may outsource or instruct the processing of personal data pertaining to a data subject;

o. "Processing" refers to any operation or any set of operations performed upon personal data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data. Processing may be performed through automated means, or manual processing, if the personal data are contained or are intended to be contained in a filing system;

p. "Profiling" refers to any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements;

q. "Privileged information" refers to any and all forms of data, which, under the Rules of Court and other pertinent laws constitute privileged communication;

r. "Public authority" refers to any government entity created by the Constitution or law, and vested with law enforcement or regulatory authority and functions;

s. "Security incident" is an event or occurrence that affects or tends to affect data protection, or may compromise the availability, integrity and confidentiality of personal data. It includes incidents that would result to a personal data breach, if not for safeguards that have been put in place;

t. Sensitive personal information refers to personal information:

1. About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;

2. About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such individual, the disposal of such proceedings, or the sentence of any court in such proceedings;

3. Issued by government agencies peculiar to an individual which includes, but is not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and

4. Specifically established by an executive order or an act of Congress to be kept classified.