Freedom of Information Manual

(Implementing Details of Executive Order No. 02 Issued on July 23, 2016 by President Rodrigo Roa Duterte)

FOREWORD

As mandated by our fundamental laws, our government has worked on the formulation and implementation of measures that will uphold the rights of the people to access information concerning government affairs. Though both delayed and suppressed due to ramifications brought by political oppression through a decade-long despotic rule, the fundamental and lawful right of citizens to information and ease of access to it have been achieved through President Rodrigo Roa Duterte's issuance of Executive Order No. 2, series 2016 (Operationalizing in the Executive Branch the People's Constitutional Right to Information and the State Policies to Full Public Disclosure and Transparency in the Public Service and Providing Guidelines Therefor).

As also aligned with the basic laws, the establishment of the mechanism under the FOI has two-pronged effects. First, it grants the people their lawful right by empowering them to an efficient and accessible means of attaining information about governmental processes and; secondly, it mandates governmental agencies and other institutions to align their policies to FOI provisions which result in a democratic exercise of conferment of what the people deserve under the tenets of integrity, transparency, and honesty.

In framing this FOI manual, the BJMP was guided by the same doctrines under the Constitution. Mindful of the need to keep the public informed of bureau practices and programs affecting the community by large, the manual thus serves as sufficient reference both for bureau personnel and citizens.

In recognition of the dictates of the laws and observance of the rights of the people, the BJMP seeks to give full effect to the requirements and goals of the FOI program with an emphasis on efficiency, timeliness, and commitment to the delivery of FOI related services.

To all personnel, who exerted time, effort, and knowledge drafting and eventual completing the BJMP FOI Manual, congratulations for a job well done and for making this resounding accomplishment a reaffirmation of our faithfulness to the laws and the people.

Thank you and Mabuhay!

JDIR ALLAN S IRAL, CESE
Chief, BJMP

22 January 2021

MESSAGE

Rights are but weapons on the wall if, like expensive tapestry, all they do is embellish and impress. It may be dormant, it might be suppressed, but sooner, or later, it will want to surface either in chaos or in peaceful assertion.

Barely more than three (3) months after the effectivity of the 1987 Constitution, the High Court in its decision2, made its first exposition relating to the right to information and ruled that the incorporation in the Constitution of a guarantee of access to information of public concern is a recognition of the essentiality of the free flow of ideas and information in a democracy.

With insistent call and so as not to view it as mere adornment, Executive Order No. 2 was promulgated institutionalizing in the Executive Branch the people's constitutional right to information and provides a mechanism for the public to get the audacity to assert it. Its assertiveness embodies a high level of consensus on the premise that an informed citizenry is essential to the existence and proper functioning democracy.

Towards this end, the BJMP-NHQ Legal Service Office coming out with the BJMP Freedom of Information (FOI) Manual as a useful reference for the BJMP personnel and the public.

For the accomplishment of this task, I commend all the personnel of the BJMP-NHQ Legal Service Office for giving their efforts and time selflessly. If not for them, this significant undertaking would not have been possible.

Thank you and more power. . .

PAULINO H MORENO, JR
Jail Senior Superintendent
Chief, Legal Service Office

09 November 2016

1Ynot v. Intermediate Appellate Court, 148 SCRA 659
2Legaspi v. CSC, G. R. No. 72119, May 29, 1987

TABLE OF CONTENTS

ANNEXES

A. Executive Order No. 02

B. Republic Act No. 10173 (Data Privacy Act of 2012)

C. List of Exceptions to FOI

D. Flow Chart

E. FOI Request Form

F. FOI Template

E. 1 FOI Receiving Officers of BJMP-NHQ and BJMP Regional Offices

E. 2 FOI Decision Makers of BJMP-NHQ and BJMP Regional Offices

E. 3. Document Enclosed

E. 4. Answer

E. 5. Document Available On-Line

E. 6. Document Not Available

E. 7. Under Exceptions

BUREAU OF JAL MANAGEMENT AND PENOLOGY (BJMP) FREEDOM OF INFORMATION (FOI) MANUAL IMPLEMENTING EXECUTIVE ORDER (EO) NO.2 ISSUED BY THE PRESIDENT WHICH OPERATIONALIZES IN THE EXECUTIVE BRANCH THE PEOPLE'S CONSTITUTIONAL RIGHT TO INFORMATION AND THE STATE POLICY TO FULL PUBLIC DISCLOSURE AND TRANSPARENCY IN THE PUBLIC SERVICE

WHEREAS, pursuant to Section 28, Article Il of the 1987 Constitution, the State adopts and implements a policy of full disclosure of all its transactions involving public interest, subject to reasonable conditions prescribed by law;

WHEREAS, Section 7, Article Ill of the Constitution guarantees the right of the people to information on matters of public concern;

WHEREAS, the incorporation of this right in the Constitution is a recognition of the fundamental role of free and open exchange of information in a democracy, meant to enhance transparency and accountability in government official acts, transactions, or decisions;

WHEREAS, the Data Privacy Act of 2012 (RA 10173), including its Implementing Rules and Regulations, strengthen the fundamental human right of privacy, and of communication while ensuring the free flow of information to promote innovation and growth;

WHEREAS, pursuant to Executive Order No. 2 issued by President RODRIGO ROA DUTERTE on 23 July 2016, the same mandates all government offices under the Executive Branch to promulgate its own Freedom of Information (FOI) Manual within one hundred twenty (120) calendar days from its effectivity;

NOW, THEREFORE, foregoing premises considered, the BJMP hereby ADOPTS and PROMULGATES the following BJMP FOI Manual pursuant to the above-cited Executive Order, to wit:

RULE 1

PRELIMINARY PROVISIONS

Section 1. Title. These Rules shall be known and cited as the "Bureau of Jail Management and Penology (BJMP) Freedom of Information (FOI) Manual or "BJMP FOI Manual" for brevity".

Section 2. Purpose. These Rules are promulgated to prescribe the procedures and guidelines to be followed by all BJMP offices in dealing with the requests for information received under Executive Order (E.O.) No. 2 on Freedom of Information (FOI). (Annex "A")

Section 3. Scope of Application. This Manual shall apply to all requests for information addressed to the BJMP National Headquarters (BJMP-NHQ) and all its Regional Offices, Jail Provincial Administrator's Offices and Jail Facilities nationwide. However, those requests which can be obtained or produced by the office concerned in the routine or regular course of business, the Anti-Red Tape Act of 2007 (RA 9485), its implementing rules and regulations and other applicable laws and rules shall apply.

RULE 11

DEFINITION OF TERMS

Section 4. Definition of Terms. For purposes of these Rules, the following terms shall mean:

a. Freedom of Information (FOI - is the right of the people to information on matters of public concern, and adopts and implements a policy of full public disclosure of all its transactions involving public interest, subject to the procedures and limitations provided in Executive Order No. 2. This right is indispensable to the exercise of the right of the people and their organizations to effective and reasonable participation at all levels of social, political and economic decision-making.

b. Information — pertains to any records, documents, papers, reports, letters, contracts, minutes and transcripts of official meetings, maps, books, photographs, data, research materials, films, sound and video recording, magnetic or other tapes, electronic data, computer stored data, any other like or similar data or materials recorded, stored or archived in whatever format, whether offline or online, which are made, received, or kept in or under the control and custody of any

government office pursuant to law, executive order, and rules and regulations or in connection with the performance or transaction of official business by any government office.

c. Information for Disclosure refers to information promoting the awareness and understanding of policies, programs, activities, rules or revisions affecting the public, government agencies, and the community and economy. It also includes information encouraging familiarity with the general operations, thrusts, and programs of the government. In line with the concept of proactive disclosure and open data, these types of information can be posted or accessed to government websites, such as data.gov.ph, without need of written requests.

d. Official Record/s - shall refer to information produced or received by a public officer or employee, or by a government office in an official capacity or pursuant to a public function or duty.

e. Open Data - refers to publicly available data structured in a way that enables the data to be fully discoverable and usable by end users.

g. Public Records - shall include information required by laws, executive orders, rules, or regulations to be entered, kept, and made publicly available by a government office.

h. Public Service Contractor - shall refer to a private entity that has dealing, contract, or a transaction of whatever form or kind with the government or a government agency or office that utilizes public funds.

i. Personal Information shall refer 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.

j. Sensitive Personal Information - As defined in the Data Privacy Act of 2012, (Annex "B") shall refer to personal information:

(1) About an individual race, ethnic origin, marital status, age, color, and religious philosophical or political affiliations;
(2) About an individual health, education, genetic or sexual life of a person, or to any proceedings for any offense committed or alleged to have committed by

such person, 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 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.

k. Frequently Requested Information - refers to information released in response to an FOI request that the BJMP determines have become or are likely to become the subject of subsequent requests for substantially the same records.

l. Full Denial - refers when the BJMP offices cannot release any records or information in response to a FOI request, because, for example, the requested information is exempt from disclosure in its entirety or no records responsive to the request could be located.

m. Full Grant - refers when the BJMP offices are able to disclose all records in full in response to an FOI request.

n. Partial Grant/Partial Denial - refers when the BJMP is able to disclose portions of the records in response to a FOI request, but deny other portions of the request.

o. Pending Request or Pending Appeal - refers to an FOI request or administrative appeal for which the BJMP offices has not yet taken final action in all respects. It captures anything that is open at a given time including requests that are well within the statutory response time.

p. Perfected Request - refers to an FOI request, which reasonably describes the records sought and is made in accordance with this Manual and other BJMP office regulations.

q. Multi-Track Processing - refers to a system that divides incoming FOI requests according to their complexity so that simple requests requiring relatively minimal review are placed in one processing track and more complex requests are placed in one or more other tracks. Requests in each track shall be acted upon or processed on a first in/first out basis.

r. Proactive Disclosure - refers to information made publicly available by the BJMP offices without waiting for a specific FOI request.

s. Processed Request or Processed Appeal refers to the number of requests or appeals made where the BJMP has completed its work and sent a final response to the requester.

t. Received Request or Received Appeal - refers to an FOI request or administrative appeal that the BJMP has received within a fiscal year.

u. Referral — refers to the process when the BJMP offices locates a record that originated with, or otherwise of primary interest of another agency, in such case, the BJMP shall forward that request to other agency to process the same and the latter shall have the final determination and shall inform the requester about the action taken.

v. Consultation — refers to the process when the BJMP locates a record that contains information of interest with another office or agency, in such case, the latter's opinion must be obtained on the disclosability of the records before any final determination is made.

w. Simple Request - refers to an FOI request which involves only a small volume of material and does not require a considerable amount of time and enables the BJMP to process the request relatively quickly.

x. data.gov.ph - refers to the open data website that serves as the government's comprehensive portal for all public government data that is searchable, understandable, and accessible.

y. eFOI.gov.ph - refers to the website that serves as the government's comprehensive FOI website for all information on the FOI. Among many other features, eFOI.gov.ph provides a central resource for the public to understand the FOI, to locate records that are already available online, and to learn how to make a request for information that is not yet publicly available. eFOI.gov.ph also promotes agency accountability for the administration of the FOI by graphically displaying the detailed statistics contained in Annual FOI Reports, so that they can be compared by agency and over time.

z. FOI Action Officer- refers to the person who assumes the responsibilities of the receiving officer in the absence of the latter including the approval or denial of the request.

RULE 111

DESIGNATION, DUTIES AND RESPONSIBILITIES OF BJMP FRO and FDM

Section 5. BJMP FOI Receiving Officer. There shall be a BJMP FOI Receiving Officer (FRO) in the BJMP National Headquarters (BJMP-NHQ) and in every BJMP Regional Offices (BJMPRO). The designated Chief, Community Relations Service Office (C, CRSO) in the National Headquarters, Chief, Regional Community Relations Service (C, RCRS) in the Regional Offices as well as the Community Relations Service Officer (CRSO) in all jail facilities shall be, during their incumbency, the BJMP FOI Receiving Officer (BJMP FRO) in their respective levels. In case the BJMP FRO is on leave or on official business where he is out of office for a number of days, the designated Officer-In-Charge (OIC) shall automatically assume the duties and responsibilities as the BJMP FRO.

Section 6. Duties of the FRO. The duties of the FRO shall include, among others, receiving on behalf of the BJMP, all requests for information, conduct initial evaluation of the request and if found sufficient, then advise the requesting party that the same shall be forwarded to the FOI Decision Maker for further evaluation.

However, the FRO may deny the request based on:

a. That the form is incomplete; or
b. That the information is already disclosed in the BJMP Official Website or at data.gov.ph.

Section 7. Monitoring of FOI Request and Appeal. The FOI Receiving Officer shall monitor all FOI requests and appeals; provide assistance to the FOI Decision Maker; provide support to the public and staff with regard to FOI; compile statistical information as required; and submit periodic report to the Chief, BJMP.

Section 8. Annual FOI Report. The FOI Receiving Officer shall prepare Annual FOI Report to be submitted and filed each year with the Presidential Communications Operations Office (PCOO). It shall contain as follows: detailed

statistics on the number of FOI requests and appeals received, processed, and pending before the BJMP-NHQ, BJMPRO and all jail stations.

Section 9. BJMP FOI Decision Maker. There shall be a BJMP FOI Decision Maker (FDM), in the BJMP-NHQ, in every BJMPRO and all jail stations nationwide. The designated Chief, Directorial Staff (CDS) in the National Headquarters, Regional Chief of Staff (RCS) in the Regional Offices and Jail Wardens in all jail stations shall be, during their incumbency, the BJMP FDM, in their respective levels. In case the BJMP FDM is on leave or on official business where h is out of office for a number of days, the designated Officer-In-Charge (OIC) shall automatically assume the duties and responsibilities as the BJMP FDM.

In instances where the CDS or RCS is holding concurrent designation as DCO or ARDA/ARDO, respectively, the Director, DPRM or the Chief, PRMD shall be designated by the Chief, BJMP or the Regional Director, as the case may be, as the FOI Decision Maker in their respective levels.

Section 10. Duties of FDM. The FOI Decision Maker shall conduct evaluation of the request for information and has the authority to grant or deny the request, based on the following:

a. That the BJMP does not have the information requested;
b. That the information requested contains sensitive personal information protected by the Data Privacy Act of 2012;
c. That the information requested falls under the list of exceptions to FOI provided for by law, rules, Executive Order and other official issuances;
d. The request is unreasonable being identical or substantially similar request from the same requesting party whose request has already been previously granted or denied by the BJMP offices; and
e. The request states NO PURPOSE/ S or if stated, it appears to be unreasonable or irrelevant as the information requested has no causal connection with the purpose.

RULE IV
PROCEDURE

Section 11. Receipt of Request for Information. The FRO shall receive the request for information from the requesting party and check compliance of the following requirements:

- The request must be in writing;
- The request shall state the name and contact number, address of the requesting party, as well as provide valid proof of identification; and
- The request shall reasonably and specifically describe the information requested, and the reason for, or purpose for which it is intended.

The request can be made through electronically, provided, that the requesting party shall attach a scanned copy of the FOI application request accompanied by a copy of a duly recognized and valid government ID with photo.

In case the requesting party is unable to make a written request, because of illiteracy or due to being a person with disability, he or she may make an oral request, and the FRO shall reduce it in writing and properly thumb marked by the requesting party.

The request shall be stamped received by the FRO, indicating the date and time of the receipt of the written request, and the name, rank, title and position of the public officer who actually received it, with a corresponding signature and a copy, furnished to the requesting party. In case of electronic requests, the same shall be printed out and shall follow the procedure mentioned above, and be, likewise, acknowledged electronically. The FRO shall input the details of the request on the Request Tracking System and allocate a reference number.

The BJMP or any of its concerned offices or stations must respond to requests promptly, within the fifteen (15) working day period following the date of receipt of the request. A working day is any day other than Saturday, Sunday, legal holiday or a day declared as national holiday by the duly constituted authorities. In computing a period, Art. 13 of the New Civil Code shall be observed.

The date of receipt of the request will either be:

a. The day on which the request is physically or electronically delivered to the government office, or directly into the email inbox of an office staff; or

b. If the government office has asked the requesting party for further details to identify and locate the requested information, the date on which the necessary clarification is received.

An exception to this is when the request has been emailed to an office staff but was not around for some reasons and this has generated an 'out of office' message with instructions on how to re-direct the message to another contact. In this case, the date of receipt will be the day the request arrives in the inbox of that contact.

Should the requested information need further details to identify or locate, then the 15 working days will commence the day after it receives the required clarification from the requesting party.

Section 12. Initial Evaluation. After receipt of the request for information, the FRO shall evaluate the contents of the request.

12.1 Request relating to more than one office under the BJMP: If a request for information is received which requires to be complied with by different Regional Offices, the FRO shall forward such request to the regional office concerned and ensure that it is well coordinated and monitor its compliance. The FRO shall make it clear with the respective offices that they will only provide the specific information that relates their office.

12.2. Requested information is not in the custody of the BJMP or any of its offices: If the requested information is not in the custody of the BJMP or any of its offices, following the referral and discussions with the FDM, the FRO shall immediately inform and advised the requesting party of such fact.

12.3. Requested information is already posted and available on-line: Should the information being requested is already posted and publicly available in the BJMP website, data.gov.ph or foi.gov.ph, the FRO shall inform the requesting party of the said fact and provide them the website link where the information is readily available.

12.4. Requested information is substantially similar or identical to the previous request: Should the requested information is substantially similar or identical to a previous request by the same

requesting party, the request shall be denied. However, the FRO shall inform the applicant of the reason of such denial.

Section 13. Transmittal of Request by FRO to the FDM. After receipt of the request for information, the FRO shall conduct initial evaluation of the information being requested, and notify the FDM of such request. A copy of the request shall be forwarded to FDM within one (1) day from receipt of the written request. The FRO shall record the date, time and name of the FDM who received the request in a record book with the corresponding signature and acknowledgement of receipt of the request.

Section 14. Role of FDM in Processing the Request. Upon receipt of the request for information from the FRO, the FDM shall assess and clarify the request if necessary. He or she shall make all necessary steps to locate and retrieve the information requested. The FDM shall ensure that the complete information requested be submitted to the FRO within 10 days upon receipt of such request.

The FRO shall note the date and time of receipt of the information from the FDM and report to the Chief, BJMP, Regional Director or Jail Warden, as the case may be, in case the ten (10) day period expires and the request still unacted upon.

If the FDM needs further details to identify or locate the information, he shall, through the FRO, seek clarification from the requesting party. The clarification shall stop the running of the 15 working day period and will commence the day after it receives the required clarification from the requesting party.

If the FDM determines that a record contains information of interest to another agency, the FDM shall consult with the agency concerned on the disclosability of the records before making any final determination.

Section 15. Role of FRO in Transmitting information to the Requesting Party. Upon receipt of the requested information from the FDM, the FRO shall collate and ensure that the information is complete. He shall attach a cover/ transmittal letter signed by the Chief, BJMP, Regional Director or Jail Warden, as the case may be, and ensure the transmittal of such information to the requesting party within 15 working days upon receipt of the request.

Section 16. Request for an Extension of Time. If the information requested requires extensive search or examination of voluminous records, or the office where the records were kept was once consumed by the occurrence of fortuitous events or other analogous circumstances, the FDM should inform the FRO and the latter shall immediately inform the requesting party of the extension, setting forth the reasons for such extension. In no case shall the extension exceed twenty (20) working days

on top of the mandated fifteen (15) working days to act on the request, unless exceptional circumstances warrant a longer period.

Section 17. Notice of Approval/ Denial of the Request. Once the FDM approved or denied the request, he shall immediately notify the FRO who shall prepare the response to the requesting party either in writing or by email.

Section 18. Approval of Request. In case of approval, the FRO shall ensure that all records that have been retrieved and considered be checked thoroughly prior to actual release. The FRO shall prepare a letter or email informing the requesting party within the prescribed period that the request was granted and be directed to pay the applicable fees, if any. All actions granting FOI requests shall pass through the Chief, BJMP, Regional Director or Jail Warden, as the case may be, for approval.

Section 19. Denial of Request. In case of denial of the request either wholly or partially, the FRO shall, within the prescribed period, notify the requesting party of the denial in writing. The notice shall clearly set forth the ground/ s of denial and the circumstances on which the denial is based. Failure to notify the requesting party of the action taken on the request within the period herein provided shall be deemed a denial of the request for information. All denials on FOI requests shall pass through the Office of the Chief, BJMP, Regional Director or Jail Warden, as the case may be, for notation.

RULE V

REMEDIES IN CASE OF DENIAL

Section 20. BJMP National Appeals and Review Committee. The BJMP National Appeals and Review Committee (NARC) is hereby duly constituted which shall be composed of three (3) Senior BJMP Commissioned Officers with the rank of at least Jail Senior Superintendent. The first two (2) members shall be the Deputy Chief for Administration (DCA), as the Chairperson and the Deputy Chief for Operations (DCO) and they remain as such during their incumbency. The third member shall be designated by the Chief, BJMP from among the Directors of the Directorates of the National Headquarters. The Community Relations Service Office shall serve as the Secretariat.

Section 21. BJMP Regional Appeals and Review Committee. The BJMP Regional Appeals and Review Committee (RARC) is hereby constituted in every Regional Office which shall be composed of the three (3) Senior BJMP Commissioned Officers in the Region. The first two (2) members shall be the Assistant Regional Director for Administration (ARDA), as the Chairperson and the

Assistant Regional Director for Operations (ARDO) and they remain as such during their incumbency. The third member shall be designated by the Regional Director from among the Division Chiefs of the Regional Office with preference to the ranking Regional Staff. The Community Relations Service of the region shall serve as the Secretariat.

Section 22. Appeal Procedure. Any person whose request for access to information has been denied by the BJMP-NHQ FDM or the BJMPRO FDM, may avail himself of the remedy set forth below:

1. Administrative FOI Appeal to the BJMPNARC/RARC: Provided, that the written appeal must be filed by the same requesting party within fifteen (15) calendar days from the notice of denial or from the lapse of the period to respond to the request.

    a. Denial of the request by the BJMP-NHQ FDM as well as denial of appeal by the BJMP Regional Appeal and Review Committee (RARC), may be appealed by filing a written appeal to the BJMP National Appeals and Review Committee (NARC) within fifteen (15) calendar days from the notice of denial of the request or appeal or from the lapse of the period to respond to the request.

    b. Denial of the request by the Regional FDM and Jail FDM, may be initially appealed to the BJMP Regional Appeals and Review Committee (RARC). Once denied, the same may be appealed to the BJMP National Appeals and Review Committee (NARC) with the same period stated above.

    c. An Appeal shall be decided by the BJMPNARC or BJMP RARC, as the case may be, within thirty (30) working days from the filing of said written appeal. Failure to decide within such period shall be deemed a denial of an appeal.

    d. The denial of an Appeal by the BJMP NARC or the lapse of the period to respond to the request may be Appealed further to the Secretary, Department of the Interior and Local Government in the same period and manner stated above.

2. Upon exhaustion of administrative FOI appeal remedies, the requesting party may file the appropriate judicial action in accordance with the Rules of Court.

RULE VI

SAFEKEEPING OF RECORDS

Section 23. Safekeeping of Records. The BJMP shall create, maintain and safely keep in appropriate places or rooms accurate and reasonably complete files, documentation or records of policies, transactions, decisions, resolutions, actions, procedures, operations, activities, communications and documents received or filed with it and the data generated or collected.

Section 24. Tracking System. The BJMP shall establish a record system using reference numbers or security bar codes to trace the status of all requests for information received by it, which may be paper-based, on-line or both.

RULE VII

PROMOTION OF OPENNESS AND PROTECTION OF PRIVACY

Section 25. Duty to Publish Information. The BJMP shall regularly publish, print and disseminate at no cost to the public and in an accessible form, in conjunction with Republic Act 9485, or the Anti-Red Tape Act of 2007, and through its website, timely, true, accurate and updated key information including, but not limited to:

a. A description of its mandate, structure, powers, functions, duties and decision-making processes;
b. A description of the frontline services it delivers and the procedure and length of time by which they may be availed of;
c. The names of its key officials, their powers, functions and responsibilities, and their profiles and curriculum vitae;
d. Work programs, development plans, investment plans, projects, performance targets and accomplishments, and budgets, revenue allotments and expenditures;
e. Important rules and regulations, orders or decisions;
f. Current and important database and statistics that it generates;
g. Bidding processes and requirements; and
h. Mechanisms or procedures by which the public may participate in or otherwise influence the formulation of policy or the exercise of its powers.

Section 26. Protection of Privacy. While providing for access to information, the BJMP shall afford full protection to a person's right to privacy, as follows:

1. The BJMP shall ensure that personal information, particularly sensitive personal information, in its custody or under its control is disclosed only as permitted by existing laws;
2. The BJMP shall protect personal information in its custody or under its control by making reasonable security arrangements against unauthorized access, leaks or premature disclosure; and
3. The FRO, FDM, or any employee or official who has access, whether authorized or unauthorized, to personal information in the custody of the BJMP shall not disclose that information except as authorized by existing laws.

RULE VIII

FEES

Section 27. No Request Fee. The BJMP shall not charge any fee for accepting requests for access to information.

Section 28. Reasonable Cost of Reproduction and Copying of the Information. The FRO shall immediately notify the requesting party in case there shall be a reproduction and copying fee in order to provide the information. Such fee shall be the actual amount spent by the BJMP in providing the information to the requesting party. The schedule of fees shall be determined and posted by the BJMP.

Section 29. Exemption from Fees. The BJMP may exempt any requesting party from payment of fees, upon request, stating therein the reason why such requesting party shall be exempt from payment of such fee.

RULE IX

ADMINISTRATIVE LIABILITY

Section 30. Non-compliance with FOI. Failure to comply with the provisions of this Manual shall be a ground for disciplinary sanction with the following administrative penalties:

a. 1st Offense - Reprimand;
b. 2nd Offense - Suspension of one (1) to thirty (30) days; and

c. 3rd Offense - Dismissal from the service.

Section 31. Disciplinary Procedure. The BJMP disciplinary machinery supplemented by the Revised Rules on Administrative Cases in the Civil Service (RRACS) shall be applicable in the disposition of cases under this Manual.

RULE X
FINAL PROVISIONS

Section 32. Separability Clause. If any provision or part of these Rules is declared invalid, the remaining provisions not affected thereby shall remain in full force and effect.

Section 33. Effectivity Clause. These Rules shall take effect upon approval and after publication in the Office of the National Administrative Register (ONAR).

PAULINO H MORENO, JR
Jail Senior Superintendent
Chief, Legal Service Office

RECOMMEND APPROVAL:

ALLAN S IRAL, CESE
Jail Chief Superintendent
Deputy Chief for Operation/
Chief Directorial Staff

DEOGRACIAS C TAPAYAI
Jail Chief Superintendent
Deputy Chief for Administr

ROVED / DISAPPROVED

SERAFIN P BARRETTO, JR. CESO IV
Jail Director
Chief, BJMP

ANNEX "A"

MALACAÑAN PALACE
MANILA

BY THE PRESIDENT OF THE PHLIPPINES

EXECUTIVE ORDER NO. 02

OPERATIONALIZING IN THE EXECUTIVE BRANCH THE PEOPLE'S CONSTITUTIONAL RIGHT TO INFORMATION AND THE STATE POLICIES TO FULL PUBLIC DISCLOSURE AND TRANSPARENCY IN PUBLIC SERVICE PROVIDING GUIDELINES THEREFOR

WHEREAS, pursuant to Article 28, Article Il of the 1987 Constitution, the State adopts and implements a policy of full public disclosure of all its transactions involving public interest, subject to reasonable conditions prescribed by law;

WHEREAS, Section 7, Article Ill of the Constitution guarantees the right of the people to information on matters of public concern;

WHEREAS, the incorporation of this right in the Constitution is a recognition of the fundamental role of free and open exchange of information in a democracy, meant to enhance transparency and accountability in government official acts, transactions, or decisions;

WHEREAS, the Executive Branch recognizes the urgent need to operationalize these Constitutional provisions;

WHEREAS, the President, under Section 17, Article VII of the Constitution, has control over all executive departments, bureaus and offices, and the duty to ensure that the laws be faithfully executed;

WHEREAS, the Data Privacy Act of 2012 (R.A. 10173), including its implementing Rules and Regulations, strengthens the fundamental human right of privacy, and of communication while ensuring the free flow of information to promote innovation and growth;

NOW, THEREFORE, 1, RODRIGO ROA DUTERTE, President of the Philippines, by virtue of the powers vested in me by the Constitution and existing laws, do hereby order:

SECTION 1. Definition. For the purpose of this Executive Order, the following terms shall mean:

(a) "Information" shall mean any records, documents, papers, reports, letters, contracts, minutes and transcripts of official meetings, maps, books, photographs, data, research materials, films, sound and video recording, magnetic or other tapes, electronic data, computer stored data, any other like or similar data or materials recorded, stored or archived in whatever format, whether offline or online, which are made, received, or kept in or under the control and custody of any government office pursuant to law, executive order, and rules and regulations or in connection with the performance or transaction of official business by any government office.

(b) "Official record/records" shall refer to information produced or received by a public officer or employee, or by a government office in an official capacity or pursuant to a public function or duty.

(c) "Public record/ records" shall include information required by laws, executive orders, rules, or regulations to be entered, kept and made publicly available by a government office.

SECTION 2. Coverage. This order shall cover all government offices under the Executive Branch, including but not limited to the national government and all its offices, departments, bureaus, offices, and instrumentalities, including government-owned or -controlled corporations, and state universities and colleges. Local government units (LGUs) are encouraged to observe and be guided by this Order.

SECTION 3. Access to information. Every Filipino shall have access to information, official records, public records and to documents and papers pertaining to official acts, transactions or decisions, as well as to government research data used as basis for policy development.

SECTION 4. Exception. Access to information shall be denied when the information falls under any of the exceptions enshrined in the Constitution, existing law or jurisprudence.

The Department of Justice and the Office of the Solicitor General are hereby directed to prepare an inventory of such exceptions and submit the same to the

Office of the President within thirty (30) calendar days from the date of effectivity of this Order.

The Office of the President shall thereafter, immediately circularize the inventory of exceptions for the guidance of all government offices and instrumentalities covered by this Order and the general public.

Said inventory of exceptions shall periodically be updated to properly reflect any change in existing law and jurisprudence and the Department of Justice and the Office of the Solicitor General are directed to update the inventory of exceptions as the need to do so arises, for circularization as hereinabove stated.

SECTION 5. Availability of SALN. Subject to the provisions contained in Sections 3 and 4 of this Order, all public officials are reminded of their obligation to file and make available for scrutiny their Statements of Assets, Liabilities and Net Worth (SALN) in accordance with existing laws, rules and regulations, and the spirit and letter of this Order.

SECTION 6. Application and Interpretation. There shall be a legal presumption in favor of access to information, public records and official records. No request for information shall be denied unless it clearly falls under any of the exceptions listed in the inventory or updated inventory of exceptions circularized by the Office of the President provided in the preceding section.
The determination of the applicability of any of the exceptions to the request shall be the responsibility of the Head of the Office, which is in custody or control of the information, public record or official record, or the responsible central or field officer duly designated by him in writing.

In making such determination, the Head of the Office or his designated officer shall exercise reasonable diligence to ensure that no exception shall be used or availed of to deny any request for information or access to public records, or official records if the denial is intended primarily and purposely to cover up a crime, wrongdoing, graft or corruption.

SECTION 7. Protection of Privacy. While providing access to information, public records, and official records, responsible officials shall afford full protection to the right to privacy of the individual as follows:

(a) Each government office per Section 2 hereof shall ensure that personal information in its custody or under its control is disclosed or released only if it is material or relevant to the subject matter of the request and its disclosure is permissible under this order or existing law, rules or regulations;

(b) Each government office must protect personal information in its custody or control by making reasonable security arrangements against leaks or premature disclosure of personal information, which unduly exposes the individual, whose personal information is requested, to vilification, harassment or any other wrongful acts.

(c) Any employee, official or director of a government office per Section 2 hereof who has access, authorized or unauthorized, to personal information in the custody of the office, must not disclose that information except when authorized under this order or pursuant to existing laws, rules or regulation.

SECTION 8. People's Freedom to Information (FOI) Manual. For the effective implementation of this Order, every government office is directed to prepare within one hundred twenty (120) calendar days from the effectivity of this Order, its own People's FOI Manual, which shall include among others the following provisions:

(a) The location and contact information of the head, regional, provincial, and field offices, and other established places where the public can obtain information or submit requests;

(b) The person or office responsible for receiving requests for information; (c) The procedure for the filing and processing of the request as specified in the succeeding section 9 of this Order.

(d) The standard forms for the submission of requests and for the proper acknowledgment of requests;

(e) The process for the disposition of requests;

(f) The procedure for the administrative appeal of any denial for access to information; and

(g) The schedule of applicable fees.

SECTION 9. Procedure. The following procedure shall govern the filing and processing of request for access to information:

(a) Any person who requests access to information shall submit a written request to the government office concerned. The request shall state the name and contact information of the requesting party, provide valid proof of his identification or authorization, reasonably describe the information requested, and the reason for, or purpose of, the request for information: Provided, that no request shall be denied or refused acceptance unless the reason for the request is contrary to law, existing rules and regulations or it is one of the exceptions contained in the inventory or updated inventory of exception as hereinabove provided.

(b) The public official receiving the request shall provide reasonable assistance, free of charge, to enable, to enable all requesting parties and

particularly those with special needs, to comply with the request requirements under this Section.

(c) The request shall be stamped by the government office, indicating the date and time of receipt and the name, rank, title and position of the receiving public officer or employee with the corresponding signature, and a copy thereof furnished to the requesting party. Each government office shall establish a system to trace the status of all requests for information received by it.

(d) The government office shall respond to a request fully compliant with requirements of sub-section (a) hereof as soon as practicable but not exceeding fifteen (15) working days from the receipt thereof. The response mentioned above refers to the decision of the agency or office concerned to grant or deny access to the information requested.

(e) The period to respond may be extended whenever the information requested requires extensive search of the government office's records facilities, examination of voluminous records, the occurrence of fortuitous cases or other analogous cases. The government office shall notify the person making the request of the extension, setting forth the reasons for such extension. In no case shall the extension go beyond twenty (20) working days unless exceptional circumstances warrant a longer period.

(f) Once a decision is made to grant the request, the person making the request shall be notified of such decision and directed to pay any applicable fees.

SECTION 10. Fees. Government offices shall not charge any fee for accepting requests for access to information. They may, however, charge a reasonable fee to reimburse necessary costs, including actual costs of reproduction and copying of the information required, subject to existing rules and regulations. In no case shall the applicable fees be so onerous as to defeat the purpose of this Order.

SECTION 11. Identical or Substantially Similar Requests. The government office shall not be required to act upon an unreasonable subsequent identical or substantially similar request from the same requesting party whose request from the same requesting party whose request has already been previously granted or denied by the same government office.

SECTION 12. Notice of Denial. If the government office decides to deny the request, in whole or in part, it shall as soon as practicable, in any case within fifteen (15) working days from the receipt of the request, notify the requesting party the denial in writing. The notice shall clearly set forth the ground or grounds for denial and the circumstances on which the denial is based. Failure to notify the requesting party of

the action taken on the request within the period herein stipulated shall be deemed a denial of the request for access to information.

SECTION 13. Remedies in Cases of Denial of Request for Access to Information.

(a) Denial of any request for access to information may be appealed to the person or office next higher in the authority, following the procedure mentioned in Section 9 of this Order: Provided, that the written appeal must be filed by the same person making the request within fifteen (15) working days from the notice of denial or from the lapse of the relevant period to respond to the request.

(b) The appeal be decided by the person or office next higher in authority within thirty (30) working days from the filing of said written appeal. Failure of such person or office to decide within the afore-stated period shall be deemed a denial of the appeal.

(c) Upon exhaustion of administrative appeal remedies, the requesting part may file the appropriate case in the proper courts in accordance with the Rules of Court.

SECTION 14. Keeping of Records. Subject to existing laws, rules, and regulations, government offices shall create and/or maintain accurate and reasonably complete records of important information in appropriate formats, and implement a records management system that facilitates easy identification, retrieval and communication of information to the public.

SECTION 15. Administrative Liability. Failure to comply with the provisions of this Order may be a ground for administrative and disciplinary sanctions against any erring public officer or employee as provided under existing laws or regulations.

SECTION 16. Implementing Details. All government offices in the Executive Branch are directed to formulate their respective implementing details taking into consideration their mandates and the nature of information in their custody or control, within one hundred twenty (120) days from the effectivity of this Order.

SECTION 17. Separability Clause. If any section or part of this Order is held unconstitutional or invalid, the other sections or provisions not otherwise affected shall remain in full force or effect.

SECTION 18. Repealing Clause. All orders, rules and regulations, issuances or any part thereof inconsistent with the provisions of this Executive Order are hereby repealed, amended or modified accordingly: Provided, that the provisions of Memorandum Circular No. 78 (s. 1964), as amended, shall not be deemed repealed pending further review.

SECTION 19. Effectivity. This Order shall take effect immediately upon publication in a newspaper of general circulation.

DONE, in the City of Manila, this 23rd day of July in the year of our Lord two thousand and sixteen.

(Sgd.) **RODRIGO ROA DUTERTE**
President of the Philippines

By the President:

(Sgd.) **SALVADOR C. MEDLALDEA**
Executive Secretary

ANNEX "B”

Republic of the Philippines
Congress of the Philippines
Metro Manila
Fifteenth Congress
Second Regular Session

Begun and held in Metro Manila, on Monday, the twenty-fifth day of July, two thousand eleven.

[REPUBLIC ACT NO. 10173]

AN ACT PROTECTING INDIVIDUAL PERSONAL INFORMATION IN INFORMATION AND COMMUNICATIONS SYSTEMS IN THE GOVERNMENT AND THE PRIVATE SECTOR, CREATING FOR THIS PURPOSE A NATIONAL PRIVACY COMMISSION, AND FOR OTHER PURPOSES

Be it enacted, by the Senate and House of Representatives of the Philippines in Congress assembled:

CHAPTER I
GENERAL PROVISIONS

SECTION 1. *Short Title.* – This Act shall be known as the “Data Privacy Act of 2012”.

SEC. 2. *Declaration of Policy.* – It is the policy of the State to protect the fundamental human right of privacy, of communication while ensuring free flow of information to promote innovation and growth. The State recognizes the vital role of information and communications technology in nation-building and its inherent obligation to ensure that personal information in information and communications systems in the government and in the private sector are secured and protected.

SEC. 3. *Definition of Terms.* – Whenever used in this Act, the following terms shall have the respective meanings hereafter set forth:

(a) *Commission* shall refer to the National Privacy Commission created by virtue of this Act.

(b) *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 personal information about and/or relating to him or her. Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of the data subject by an agent specifically authorized by the data subject to do so.

(c) *Data subject* refers to an individual whose personal information is processed.

(d) *Direct marketing* refers to communication by whatever means of any advertising or marketing material which is directed to particular individuals.

(e) *Filing system* refers to any act 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 person is readily accessible.

(f) *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 or 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.

(g) *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.

(h) *Personal information controller* refers to a person or organization who controls the collection, holding, processing or use of personal information, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf. The term excludes:

(1) A person or organization who performs such functions as instructed by another person or organization; and

(2) An individual who collects, holds, processes or uses personal information in connection with the individual’s personal, family or household affairs.

(i) *Personal information processor* refers to any natural or juridical person qualified to act as such under this Act to whom a personal information controller may outsource the processing of personal data pertaining to a data subject.

(j) *Processing* refers to any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.

(k) *Privileged information* refers to any and all forms of data which under the Rules of Court and other pertinent laws constitute privileged communication.

(l) *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 person, 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 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.

SEC. 4. *Scope.* – This Act applies to the processing of all types of personal information and to any natural and juridical person involved in personal information processing including those personal information controllers and processors who, although not found or established in the Philippines, use equipment that are located in the Philippines, or those who maintain an office, branch or agency in the Philippines subject to the immediately succeeding paragraph: *Provided,* That the requirements of Section 5 are complied with.

This Act does not apply to the following:

(a) Information about any individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual, including:

(1) The fact that the individual is or was an officer or employee of the government institution;

(2) The title, business address and office telephone number of the individual;

(3) The classification, salary range and responsibilities of the position held by the individual; and

(4) The name of the individual on a document prepared by the individual in the course of employment with the government;

(b) Information about an individual who is or was performing service under contract for a government institution that relates to the services performed, including the terms of the contract, and the name of the individual given in the course of the performance of those services;

(c) Information relating to any discretionary benefit of a financial nature such as the granting of a license or permit given by the government to an individual, including the name of the individual and the exact nature of the benefit;

(d) Personal information processed for journalistic, artistic, literary or research purposes;

(e) Information necessary in order to carry out the functions of public authority which includes the processing of personal data for the performance by the independent, central monetary authority and law enforcement and regulatory agencies of their constitutionally and statutorily mandated functions. Nothing in this Act shall be construed as to have amended or repealed Republic Act No. 1405, otherwise known as the Secrecy of Bank Deposits Act; Republic Act No. 6426, otherwise known as the Foreign Currency Deposit Act; and Republic Act No. 9510, otherwise known as the Credit Information System Act (CISA);

(f) Information necessary for banks and other financial institutions under the jurisdiction of the independent, central monetary authority or Bangko Sentral ng Pilipinas to comply with Republic Act No. 9510, and Republic Act No. 9160, as amended, otherwise known as the Anti-Money Laundering Act and other applicable laws; and

(g) Personal information originally collected from residents of foreign jurisdictions in accordance with the laws of those foreign jurisdictions, including any applicable data privacy laws, which is being processed in the Philippines.

SEC. 5. *Protection Afforded to Journalists and Their Sources.* – Nothing in this Act shall be construed as to have amended or repealed the provisions of Republic Act No. 53, which affords the publishers, editors or duly accredited reporters of any newspaper, magazine or periodical of general circulation protection from being compelled to reveal the source of any news report or information appearing in said publication which was related in any confidence to such publisher, editor, or reporter.

SEC. 6. *Extraterritorial Application.* – This Act applies to an act done or practice engaged in and outside of the Philippines by an entity if:

(a) The act, practice or processing relates to personal information about a Philippine citizen or a resident;

(b) The entity has a link with the Philippines, and the entity is processing personal information in the Philippines or even if the processing is outside the Philippines as long as it is about Philippine citizens or residents such as, but not limited to, the following:

(1) A contract is entered in the Philippines;

(2) A juridical entity unincorporated in the Philippines but has central management and control in the country; and

(3) An entity that has a branch, agency, office or subsidiary in the Philippines and the parent or affiliate of the Philippine entity has access to personal information; and

(c) The entity has other links in the Philippines such as, but not limited to:

(1) The entity carries on business in the Philippines; and

(2) The personal information was collected or held by an entity in the Philippines.

CHAPTER II
THE NATIONAL PRIVACY COMMISSION

SEC. 7. *Functions of the National Privacy Commission.* – To administer and implement the provisions of this Act, and to monitor and ensure compliance of the country with international standards set for data protection, there is hereby created an independent

body to be known as the National Privacy Commission, winch shall have the following functions:

(a) Ensure compliance of personal information controllers with the provisions of this Act;

(b) Receive complaints, institute investigations, facilitate or enable settlement of complaints through the use of alternative dispute resolution processes, adjudicate, award indemnity on matters affecting any personal information, prepare reports on disposition of complaints and resolution of any investigation it initiates, and, in cases it deems appropriate, publicize any such report: *Provided,* That in resolving any complaint or investigation (except where amicable settlement is reached by the parties), the Commission shall act as a collegial body. For this purpose, the Commission may be given access to personal information that is subject of any complaint and to collect the information necessary to perform its functions under this Act;

(c) Issue cease and desist orders, impose a temporary or permanent ban on the processing of personal information, upon finding that the processing will be detrimental to national security and public interest;

(d) Compel or petition any entity, government agency or instrumentality to abide by its orders or take action on a matter affecting data privacy;

(e) Monitor the compliance of other government agencies or instrumentalities on their security and technical measures and recommend the necessary action in order to meet minimum standards for protection of personal information pursuant to this Act;

(f) Coordinate with other government agencies and the private sector on efforts to formulate and implement plans and policies to strengthen the protection of personal information in the country;

(g) Publish on a regular basis a guide to all laws relating to data protection;

(h) Publish a compilation of agency system of records and notices, including index and other finding aids;

(i) Recommend to the Department of Justice (DOJ) the prosecution and imposition of penalties specified in Sections 25 to 29 of this Act;

(j) Review, approve, reject or require modification of privacy codes voluntarily adhered to by personal information controllers: *Provided,* That the privacy codes shall adhere to

the underlying data privacy principles embodied in this Act: *Provided, further,* That such privacy codes may include private dispute resolution mechanisms for complaints against any participating personal information controller. For this purpose, the Commission shall consult with relevant regulatory agencies in the formulation and administration of privacy codes applying the standards set out in this Act, with respect to the persons, entities, business activities and business sectors that said regulatory bodies are authorized to principally regulate pursuant to the law: *Provided, finally.* That the Commission may review such privacy codes and require changes thereto for purposes of complying with this Act;

(k) Provide assistance on matters relating to privacy or data protection at the request of a national or local agency, a private entity or any person;

(l) Comment on the implication on data privacy of proposed national or local statutes, regulations or procedures, issue advisory opinions and interpret the provisions of this Act and other data privacy laws;

(m) Propose legislation, amendments or modifications to Philippine laws on privacy or data protection as may be necessary;

(n) Ensure proper and effective coordination with data privacy regulators in other countries and private accountability agents, participate in international and regional initiatives for data privacy protection;

(o) Negotiate and contract with other data privacy authorities of other countries for cross-border application and implementation of respective privacy laws;

(p) Assist Philippine companies doing business abroad to respond to foreign privacy or data protection laws and regulations; and

(q) Generally perform such acts as may be necessary to facilitate cross-border enforcement of data privacy protection.

SEC. 8. *Confidentiality.* – The Commission shall ensure at all times the confidentiality of any personal information that comes to its knowledge and possession.

SEC. 9. *Organizational Structure of the Commission.* – The Commission shall be attached to the Department of Information and Communications Technology (DICT) and shall be headed by a Privacy Commissioner, who shall also act as Chairman of the Commission. The Privacy Commissioner shall be assisted by two (2) Deputy Privacy Commissioners, one to be responsible for Data Processing Systems and one to be

responsible for Policies and Planning. The Privacy Commissioner and the two (2) Deputy Privacy Commissioners shall be appointed by the President of the Philippines for a term of three (3) years, and may be reappointed for another term of three (3) years. Vacancies in the Commission shall be filled in the same manner in which the original appointment was made.

The Privacy Commissioner must be at least thirty-five (35) years of age and of good moral character, unquestionable integrity and known probity, and a recognized expert in the field of information technology and data privacy. The Privacy Commissioner shall enjoy the benefits, privileges and emoluments equivalent to the rank of Secretary.

The Deputy Privacy Commissioners must be recognized experts in the field of information and communications technology and data privacy. They shall enjoy the benefits, privileges and emoluments equivalent to the rank of Undersecretary.

The Privacy Commissioner, the Deputy Commissioners, or any person acting on their behalf or under their direction, shall not be civilly liable for acts done in good faith in the performance of their duties. However, he or she shall be liable for willful or negligent acts done by him or her which are contrary to law, morals, public policy and good customs even if he or she acted under orders or instructions of superiors: *Provided,* That in case a lawsuit is filed against such official on the subject of the performance of his or her duties, where such performance is lawful, he or she shall be reimbursed by the Commission for reasonable costs of litigation.

SEC. 10. *The Secretariat.* – The Commission is hereby authorized to establish a Secretariat. Majority of the members of the Secretariat must have served for at least five (5) years in any agency of the government that is involved in the processing of personal information including, but not limited to, the following offices: Social Security System (SSS), Government Service Insurance System (GSIS), Land Transportation Office (LTO), Bureau of Internal Revenue (BIR), Philippine Health Insurance Corporation (PhilHealth), Commission on Elections (COMELEC), Department of Foreign Affairs (DFA), Department of Justice (DOJ), and Philippine Postal Corporation (Philpost).

CHAPTER III
PROCESSING OF PERSONAL INFORMATION

SEC. 11. *General Data Privacy Principles.* – The processing of personal information shall be allowed, subject to compliance with the requirements of this Act and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and proportionality.

Personal information must, be:,

(a) Collected for specified and legitimate purposes determined and declared before, or as soon as reasonably practicable after collection, and later processed in a way compatible with such declared, specified and legitimate purposes only;

(b) Processed fairly and lawfully;

(c) Accurate, relevant and, where necessary for purposes for which it is to be used the processing of personal information, kept up to date; inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing restricted;

(d) Adequate and not excessive in relation to the purposes for which they are collected and processed;

(e) Retained only for as long as necessary for the fulfillment of the purposes for which the data was obtained or for the establishment, exercise or defense of legal claims, or for legitimate business purposes, or as provided by law; and

(f) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected and processed: *Provided,* That personal information collected for other purposes may lie processed for historical, statistical or scientific purposes, and in cases laid down in law may be stored for longer periods: *Provided, further,*That adequate safeguards are guaranteed by said laws authorizing their processing.

The personal information controller must ensure implementation of personal information processing principles set out herein.

SEC. 12. *Criteria for Lawful Processing of Personal Information.* – The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists:

(a) The data subject has given his or her consent;

(b) The processing of personal information is necessary and is related to the fulfillment of a contract with the data subject or in order to take steps at the request of the data subject prior to entering into a contract;

(c) The processing is necessary for compliance with a legal obligation to which the personal information controller is subject;

(d) The processing is necessary to protect vitally important interests of the data subject, including life and health;

(e) The processing is necessary in order to respond to national emergency, to comply with the requirements of public order and safety, or to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate; or

(f) The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.

SEC. 13. *Sensitive Personal Information and Privileged Information.* – The processing of sensitive personal information and privileged information shall be prohibited, except in the following cases:

(a) The data subject has given his or her consent, specific to the purpose prior to the processing, or in the case of privileged information, all parties to the exchange have given their consent prior to processing;

(b) The processing of the same is provided for by existing laws and regulations: *Provided,* That such regulatory enactments guarantee the protection of the sensitive personal information and the privileged information: *Provided, further,* That the consent of the data subjects are not required by law or regulation permitting the processing of the sensitive personal information or the privileged information;

(c) The processing is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his or her consent prior to the processing;

(d) The processing is necessary to achieve the lawful and noncommercial objectives of public organizations and their associations: *Provided,* That such processing is only confined and related to the *bona fide* members of these organizations or their associations: *Provided, further,* That the sensitive personal information are not transferred to third parties: *Provided, finally,* That consent of the data subject was obtained prior to processing;

(e) The processing is necessary for purposes of medical treatment, is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal information is ensured; or

(f) The processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or public authority.

SEC. 14. *Subcontract of Personal Information.* – *A* personal information controller may subcontract the processing of personal information: *Provided,* That the personal information controller shall be responsible for ensuring that proper safeguards are in place to ensure the confidentiality of the personal information processed, prevent its use for unauthorized purposes, and generally, comply with the requirements of this Act and other laws for processing of personal information. The personal information processor shall comply with all the requirements of this Act and other applicable laws.

SEC. 15. *Extension of Privileged Communication.* – Personal information controllers may invoke the principle of privileged communication over privileged information that they lawfully control or process. Subject to existing laws and regulations, any evidence gathered on privileged information is inadmissible.

CHAPTER IV
RIGHTS OF THE DATA SUBJECT

SEC. 16. *Rights of the Data Subject.* – The data subject is entitled to:

(a) Be informed whether personal information pertaining to him or her shall be, are being or have been processed;

(b) Be furnished the information indicated hereunder before the entry of his or her personal information into the processing system of the personal information controller, or at the next practical opportunity:

(1) Description of the personal information to be entered into the system;

(2) Purposes for which they are being or are to be processed;

(3) Scope and method of the personal information processing;

(4) The recipients or classes of recipients to whom they are or may be disclosed;

(5) Methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized;

(6) The identity and contact details of the personal information controller or its representative;

(7) The period for which the information will be stored; and

(8) The existence of their rights, i.e., to access, correction, as well as the right to lodge a complaint before the Commission.

Any information supplied or declaration made to the data subject on these matters shall not be amended without prior notification of data subject: *Provided*, That the notification under subsection (b) shall not apply should the personal information be needed pursuant to a *subpoena* or when the collection and processing are for obvious purposes, including when it is necessary for the performance of or in relation to a contract or service or when necessary or desirable in the context of an employer-employee relationship, between the collector and the data subject, or when the information is being collected and processed as a result of legal obligation;

(c) Reasonable access to, upon demand, the following:

(1) Contents of his or her personal information that were processed;

(2) Sources from which personal information were obtained;

(3) Names and addresses of recipients of the personal information;

(4) Manner by which such data were processed;

(5) Reasons for the disclosure of the personal information to recipients;

(6) Information on automated processes where the data will or likely to be made as the sole basis for any decision significantly affecting or will affect the data subject;

(7) Date when his or her personal information concerning the data subject were last accessed and modified; and

(8) The designation, or name or identity and address of the personal information controller;

(d) Dispute the inaccuracy or error in the personal information and have the personal information controller correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable. If the personal information have been corrected, the personal information controller shall ensure the accessibility of both the new and the

retracted information and the simultaneous receipt of the new and the retracted information by recipients thereof: *Provided,* That the third parties who have previously received such processed personal information shall he informed of its inaccuracy and its rectification upon reasonable request of the data subject;

(e) Suspend, withdraw or order the blocking, removal or destruction of his or her personal information from the personal information controller's filing system upon discovery and substantial proof that the personal information are incomplete, outdated, false, unlawfully obtained, used for unauthorized purposes or are no longer necessary for the purposes for which they were collected. In this case, the personal information controller may notify third parties who have previously received such processed personal information; and

(f) Be indemnified for any damages sustained due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal information.

SEC. 17. *Transmissibility of Rights of the Data Subject.* – The lawful heirs and assigns of the data subject may invoke the rights of the data subject for, which he or she is an heir or assignee at any time after the death of the data subject or when the data subject is incapacitated or incapable of exercising the rights as enumerated in the immediately preceding section.

SEC. 18. *Right to Data Portability.* – The data subject shall have the right, where personal information is processed by electronic means and in a structured and commonly used format, to obtain from the personal information controller a copy of data undergoing processing in an electronic or structured format, which is commonly used and allows for further use by the data subject. The Commission may specify the electronic format referred to above, as well as the technical standards, modalities and procedures for their transfer.

SEC. 19. *Non-Applicability.* – The immediately preceding sections are not applicable if the processed personal information are used only for the needs of scientific and statistical research and, on the basis of such, no activities are carried out and no decisions are taken regarding the data subject: *Provided,* That the personal information shall be held under strict confidentiality and shall be used only for the declared purpose. Likewise, the immediately preceding sections are not applicable to processing of personal information gathered for the purpose of investigations in relation to any criminal, administrative or tax liabilities of a data subject.

CHAPTER V
SECURITY OF PERSONAL INFORMATION

SEC. 20. *Security of Personal Information.* – (a) The personal information controller must implement reasonable and appropriate organizational, physical and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing.

(b) The personal information controller shall implement reasonable and appropriate measures to protect personal information against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination.

(c) The determination of the appropriate level of security under this section must take into account the nature of the personal information to be protected, the risks represented by the processing, the size of the organization and complexity of its operations, current data privacy best practices and the cost of security implementation. Subject to guidelines as the Commission may issue from time to time, the measures implemented must include:

(1) Safeguards to protect its computer network against accidental, unlawful or unauthorized usage or interference with or hindering of their functioning or availability;

(2) A security policy with respect to the processing of personal information;

(3) A process for identifying and accessing reasonably foreseeable vulnerabilities in its computer networks, and for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach; and

(4) Regular monitoring for security breaches and a process for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach.

(d) The personal information controller must further ensure that third parties processing personal information on its behalf shall implement the security measures required by this provision.

(e) The employees, agents or representatives of a personal information controller who are involved in the processing of personal information shall operate and hold personal information under strict confidentiality if the personal information are not intended for

public disclosure. This obligation shall continue even after leaving the public service, transfer to another position or upon termination of employment or contractual relations.

(f) The personal information controller shall promptly notify the Commission and affected data subjects when sensitive personal information or other information that may, under the circumstances, be used to enable identity fraud are reasonably believed to have been acquired by an unauthorized person, and the personal information controller or the Commission believes (bat such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject. The notification shall at least describe the nature of the breach, the sensitive personal information possibly involved, and the measures taken by the entity to address the breach. Notification may be delayed only to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system.

(1) In evaluating if notification is unwarranted, the Commission may take into account compliance by the personal information controller with this section and existence of good faith in the acquisition of personal information.

(2) The Commission may exempt a personal information controller from notification where, in its reasonable judgment, such notification would not be in the public interest or in the interests of the affected data subjects.

(3) The Commission may authorize postponement of notification where it may hinder the progress of a criminal investigation related to a serious breach.

CHAPTER VI
ACCOUNTABILITY FOR TRANSFER OF PERSONAL INFORMATION

SEC. 21. *Principle of Accountability.* – Each personal information controller is responsible for personal information under its control or custody, including information that have been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation.

(a) The personal information controller is accountable for complying with the requirements of this Act and shall use contractual or other reasonable means to provide a comparable level of protection while the information are being processed by a third party.

(b) The personal information controller shall designate an individual or individuals who are accountable for the organization's compliance with this Act. The identity of the individual(s) so designated shall be made known to any data subject upon request.

CHAPTER VII
SECURITY OF SENSITIVE PERSONAL INFORMATION IN GOVERNMENT

SEC. 22. *Responsibility of Heads of Agencies.* – All sensitive personal information maintained by the government, its agencies and instrumentalities shall be secured, as far as practicable, with the use of the most appropriate standard recognized by the information and communications technology industry, and as recommended by the Commission. The head of each government agency or instrumentality shall be responsible for complying with the security requirements mentioned herein while the Commission shall monitor the compliance and may recommend the necessary action in order to satisfy the minimum standards.

SEC. 23. *Requirements Relating to Access by Agency Personnel to Sensitive Personal Information.* – (a) On-site and Online Access – Except as may be allowed through guidelines to be issued by the Commission, no employee of the government shall have access to sensitive personal information on government property or through online facilities unless the employee has received a security clearance from the head of the source agency.

(b) Off-site Access – Unless otherwise provided in guidelines to be issued by the Commission, sensitive personal information maintained by an agency may not be transported or accessed from a location off government property unless a request for such transportation or access is submitted and approved by the head of the agency in accordance with the following guidelines:

(1) Deadline for Approval or Disapproval – In the case of any request submitted to the head of an agency, such head of the agency shall approve or disapprove the request within two (2) business days after the date of submission of the request. In case there is no action by the head of the agency, then such request is considered disapproved;

(2) Limitation to One thousand (1,000) Records – If a request is approved, the head of the agency shall limit the access to not more than one thousand (1,000) records at a time; and

(3) Encryption – Any technology used to store, transport or access sensitive personal information for purposes of off-site access approved under this subsection shall be

secured by the use of the most secure encryption standard recognized by the Commission.

The requirements of this subsection shall be implemented not later than six (6) months after the date of the enactment of this Act.

SEC. 24. *Applicability to Government Contractors.* – In entering into any contract that may involve accessing or requiring sensitive personal information from one thousand (1,000) or more individuals, an agency shall require a contractor and its employees to register their personal information processing system with the Commission in accordance with this Act and to comply with the other provisions of this Act including the immediately preceding section, in the same manner as agencies and government employees comply with such requirements.

CHAPTER VIII
PENALTIES

SEC. 25. *Unauthorized Processing of Personal Information and Sensitive Personal Information.* – (a) The unauthorized processing of personal information shall be penalized by imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00) shall be imposed on persons who process personal information without the consent of the data subject, or without being authorized under this Act or any existing law.

(b) The unauthorized processing of personal sensitive information shall be penalized by imprisonment ranging from three (3) years to six (6) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Four million pesos (Php4,000,000.00) shall be imposed on persons who process personal information without the consent of the data subject, or without being authorized under this Act or any existing law.

SEC. 26. *Accessing Personal Information and Sensitive Personal Information Due to Negligence.* – (a) Accessing personal information due to negligence shall be penalized by imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00) shall be imposed on persons who, due to negligence, provided access to personal information without being authorized under this Act or any existing law.

(b) Accessing sensitive personal information due to negligence shall be penalized by imprisonment ranging from three (3) years to six (6) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Four million pesos (Php4,000,000.00) shall be imposed on persons who, due to negligence, provided access to personal information without being authorized under this Act or any existing law.

SEC. 27. *Improper Disposal of Personal Information and Sensitive Personal Information.* – (a) The improper disposal of personal information shall be penalized by imprisonment ranging from six (6) months to two (2) years and a fine of not less than One hundred thousand pesos (Php100,000.00) but not more than Five hundred thousand pesos (Php500,000.00) shall be imposed on persons who knowingly or negligently dispose, discard or abandon the personal information of an individual in an area accessible to the public or has otherwise placed the personal information of an individual in its container for trash collection.

(b) The improper disposal of sensitive personal information shall be penalized by imprisonment ranging from one (1) year to three (3) years and a fine of not less than One hundred thousand pesos (Php100,000.00) but not more than One million pesos (Php1,000,000.00) shall be imposed on persons who knowingly or negligently dispose, discard or abandon the personal information of an individual in an area accessible to the public or has otherwise placed the personal information of an individual in its container for trash collection.

SEC. 28. *Processing of Personal Information and Sensitive Personal Information for Unauthorized Purposes.* – The processing of personal information for unauthorized purposes shall be penalized by imprisonment ranging from one (1) year and six (6) months to five (5) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00) shall be imposed on persons processing personal information for purposes not authorized by the data subject, or otherwise authorized under this Act or under existing laws.

The processing of sensitive personal information for unauthorized purposes shall be penalized by imprisonment ranging from two (2) years to seven (7) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00) shall be imposed on persons processing sensitive personal information for purposes not authorized by the data subject, or otherwise authorized under this Act or under existing laws.

SEC. 29. *Unauthorized Access or Intentional Breach.* – The penalty of imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred

thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00) shall be imposed on persons who knowingly and unlawfully, or violating data confidentiality and security data systems, breaks in any way into any system where personal and sensitive personal information is stored.

SEC. 30. *Concealment of Security Breaches Involving Sensitive Personal Information.* – The penalty of imprisonment of one (1) year and six (6) months to five (5) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00) shall be imposed on persons who, after having knowledge of a security breach and of the obligation to notify the Commission pursuant to Section 20(f), intentionally or by omission conceals the fact of such security breach.

SEC. 31. *Malicious Disclosure.* – Any personal information controller or personal information processor or any of its officials, employees or agents, who, with malice or in bad faith, discloses unwarranted or false information relative to any personal information or personal sensitive information obtained by him or her, shall be subject to imprisonment ranging from one (1) year and six (6) months to five (5) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00).

SEC. 32. *Unauthorized Disclosure.* – (a) Any personal information controller or personal information processor or any of its officials, employees or agents, who discloses to a third party personal information not covered by the immediately preceding section without the consent of the data subject, shall he subject to imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00).

(b) Any personal information controller or personal information processor or any of its officials, employees or agents, who discloses to a third party sensitive personal information not covered by the immediately preceding section without the consent of the data subject, shall be subject to imprisonment ranging from three (3) years to five (5) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00).

SEC. 33. *Combination or Series of Acts.* – Any combination or series of acts as defined in Sections 25 to 32 shall make the person subject to imprisonment ranging from three (3) years to six (6) years and a fine of not less than One million pesos (Php1,000,000.00) but not more than Five million pesos (Php5,000,000.00).

SEC. 34. *Extent of Liability.* – If the offender is a corporation, partnership or any juridical person, the penalty shall be imposed upon the responsible officers, as the case may be, who participated in, or by their gross negligence, allowed the commission of the crime. If the offender is a juridical person, the court may suspend or revoke any of its rights under this Act. If the offender is an alien, he or she shall, in addition to the penalties herein prescribed, be deported without further proceedings after serving the penalties prescribed. If the offender is a public official or employee and lie or she is found guilty of acts penalized under Sections 27 and 28 of this Act, he or she shall, in addition to the penalties prescribed herein, suffer perpetual or temporary absolute disqualification from office, as the case may be.

SEC. 35. *Large-Scale.* – The maximum penalty in the scale of penalties respectively provided for the preceding offenses shall be imposed when the personal information of at least one hundred (100) persons is harmed, affected or involved as the result of the above mentioned actions.

SEC. 36. *Offense Committed by Public Officer.* – When the offender or the person responsible for the offense is a public officer as defined in the Administrative Code of the Philippines in the exercise of his or her duties, an accessory penalty consisting in the disqualification to occupy public office for a term double the term of criminal penalty imposed shall he applied.

SEC. 37. *Restitution.* – Restitution for any aggrieved party shall be governed by the provisions of the New Civil Code.

CHAPTER IX
MISCELLANEOUS PROVISIONS

SEC. 38. *Interpretation.* – Any doubt in the interpretation of any provision of this Act shall be liberally interpreted in a manner mindful of the rights and interests of the individual about whom personal information is processed.

SEC. 39. *Implementing Rules and Regulations (IRR).* – Within ninety (90) days from the effectivity of this Act, the Commission shall promulgate the rules and regulations to effectively implement the provisions of this Act.

SEC. 40. *Reports and Information.* – The Commission shall annually report to the President and Congress on its activities in carrying out the provisions of this Act. The Commission shall undertake whatever efforts it may determine to be necessary or appropriate to inform and educate the public of data privacy, data protection and fair information rights and responsibilities.

SEC. 41. *Appropriations Clause.* – The Commission shall be provided with an initial appropriation of Twenty million pesos (Php20,000,000.00) to be drawn from the national government. Appropriations for the succeeding years shall be included in the General Appropriations Act. It shall likewise receive Ten million pesos (Php10,000,000.00) per year for five (5) years upon implementation of this Act drawn from the national government.

SEC. 42. *Transitory Provision.* – Existing industries, businesses and offices affected by the implementation of this Act shall be given one (1) year transitory period from the effectivity of the IRR or such other period as may be determined by the Commission, to comply with the requirements of this Act.

In case that the DICT has not yet been created by the time the law takes full force and effect, the National Privacy Commission shall be attached to the Office of the President.

SEC. 43. *Separability Clause.* – If any provision or part hereof is held invalid or unconstitutional, the remainder of the law or the provision not otherwise affected shall remain valid and subsisting.

SEC. 44. *Repealing Clause.* – The provision of Section 7 of Republic Act No. 9372, otherwise known as the "Human Security Act of 2007", is hereby amended. Except as otherwise expressly provided in this Act, all other laws, decrees, executive orders, proclamations and administrative regulations or parts thereof inconsistent herewith are hereby repealed or modified accordingly.

SEC. 45. *Effectivity Clause.* – This Act shall take effect fifteen (15) days after its publication in at least two (2) national newspapers of general circulation.

(Sgd.) **FELICIANO BELMONTE JR.** *Speaker of the House of Representatives*

(Sgd.) **JUAN PONCE ENRILE** *President of the Senate*

This Act which is a consolidation of Senate Bill No. 2965 and House Bill No. 4115 was finally passed by the Senate and the House of Representatives on June 6, 2012.

(Sgd.) **MARILYN B. BARUA-YAP** *Secretary General House of Representatives*

(Sgd.) **EMMA LIRIO-REYES** *Secretary of the Senate*

Approved: **AUG 15 2012**

(Sgd.) **BENIGNO S. AQUINO III** *President of the Philippines*

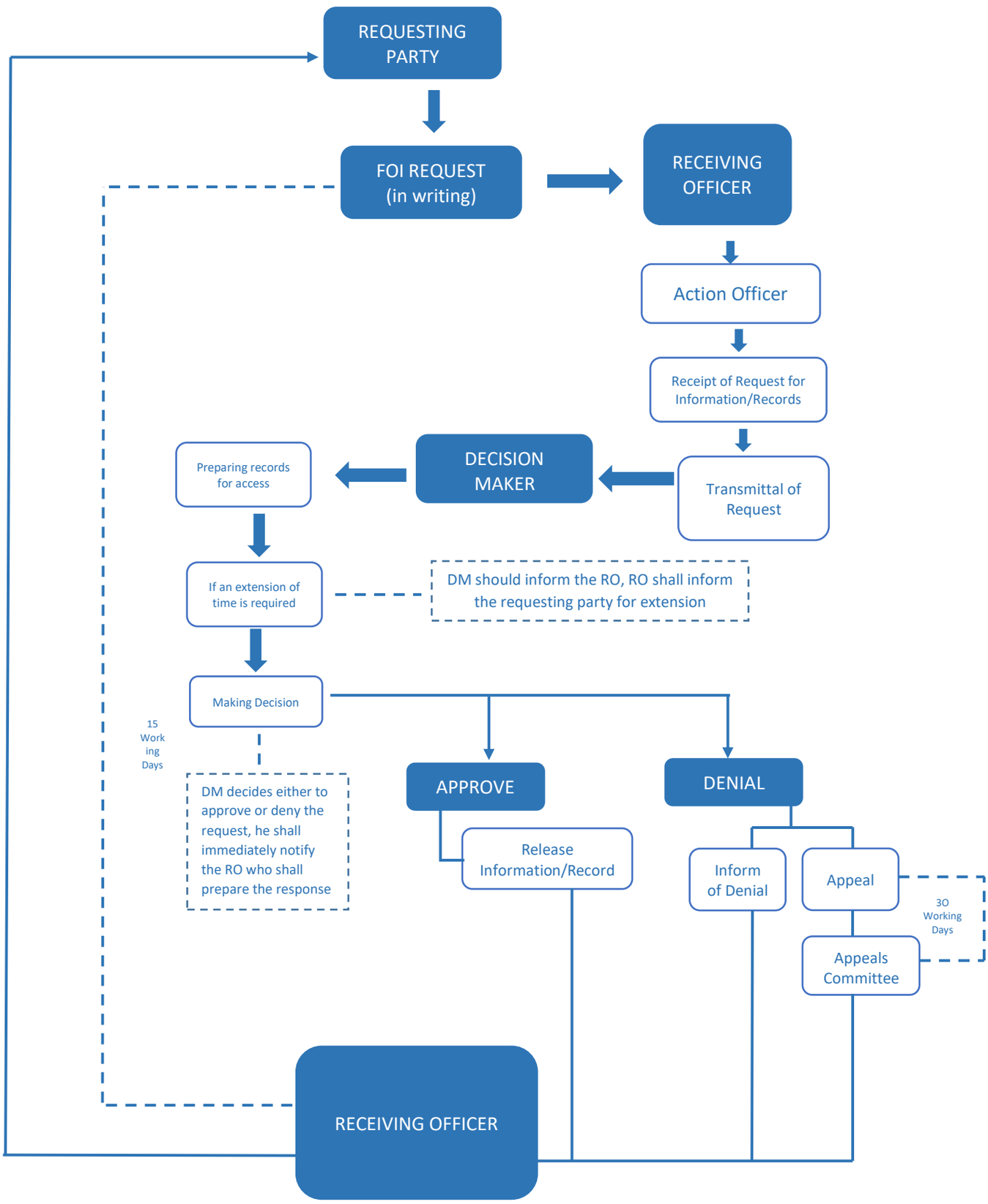
ANNEX “C”

LIST OF EXCEPTIONS

<To be provided by the Office of the Executive Secretary>

ANNEX “D”

FOI Request Flow Chart



ANNEX "E"

(Name of Office)
(Address of the Office)

PORMULARYO NG KAHILINGAN (FOI)
FOI Request Form

TITULO NG DOKUMENTO I (Title ofthe Document): _____
MGA TAON/PANAHONG SAKI-AW 1 (Year): _____
LAYUNIN 1 (Purpose):

_____

_____

_____

PANGALAN 1 (Name): _____ CONTACT Nos. _____
LAGDA I (Signature): _____ PETSA 1 (Date): _____
TIRAHAN 1 (Address): _____ KATIBAYAN NG PAGKAKAKILANLAN/(Proof of Identity):
PARAAN NG PAGTANGGAP NG IMPORMASYON/ Passport No. (How would you like to receive the information?) Drivers License _____

- ☐ Email _____
- ☐ Fax _____
- ☐ Postal Address _____
- ☐ Pick-up*(Office hours)* _____

Other

Gawaingitinalagakay: _____
(Submitted to) (Lumagdasaibabangpangalangnakalimbag) Petsa/OrasngPagkatalaga:

_____
(Date / Time of Submission)
TaongnagpapatunayngGawaingNatapos: _____
(Certified by) _____
(Lumagdasaibabangpangalangnakalimbag)

Uri ngisinagawangaksiyon: _____
(Type of action conducted)

Tinanggapni I (Received by):

_____
FOI Receiving Officer

Remarks:

_____

ANNEX "F-1"

FOI Receiving Officers of the BJMP-NHQ and BJMPRO and Jail Stations

Name of Office	Location of FOI Receiving Office	Contact Details	Assigned FOI Receiving Officer

ANNEX "F-2"

FOI Decision Makers of the BJMP-NHQ,
BJMPRO and Jail Stations

Name of Office	Location of FOI Receiving Office	Contact Details	Assigned FOI Receiving Officer

ANNEX "F-3"

FOI TEMPLATE - DOCUMENT ENCLOSED

DATE

Dear_____,

Greetings!

Thank you for your request dated <insert data> under Executive Order No. 2 (s. 2016) on Freedom of Information in the Executive Branch.

Your request

You asked for <quote request exactly, unless it is too long/complicated>.

Response to your request

Your FOI request is approved. I enclose a copy of (some/most/all* of the information you requested [in the format you asked for)

Thank you.

Respectfully,

_____

FOI Receiving Officer

ANNEX "F-4"

FOI RESPONSE TEMPLATE - ANSWER

DATE

Dear_____,

Greetings!

Thank you for your request dated <insert data> under Executive Order No. 2 (s. 2016) on Freedom of Information in the Executive Branch.

Your request

You asked for <quote request exactly, unless it is too long/complicated>.

Response to your request

Your FOI request is approved. The answer to your request is <insert answer>

Thank you.

Respectfully,

_____

FOI Receiving Officer

ANNEX "F-5"

FOI RESPONSE TEMPLATE - DOCUMENT AVAILABLE ONLINE

DATE

Dear_____,

Greetings!

Thank you for your request dated <insert data> under Executive Order No. 2 (s. 2016) on Freedom of Information in the Executive Branch.

Your request

You asked for <quote request exactly, unless it is too long/complicated>.

Response to your request

[Some/Most/Alll of the information you have requested is already available online from <add details of where that specific information can be obtained e.g. data.gov.ph, foi.gov.ph or other government websites>.

Your right to request a review

If you are unhappy with this response to your FOI request, you may ask us to carry out an internal review of the response, by writing to <insert name of Chief, BJMP, or the RD, as the case may be, and postal / e-mail address>. Your review request should explain why you are dissatisfied with this response, and should be made within 15 calendar days from the date when you received this letter. We will complete the review and tell you the result, within 30 calendar days from the date when we receive your review request.

If you are not satisfied with result of the review, you then have the right to appeal to the BJMP Central Appeal and Review Committee pursuant to BJMP FOI Manual.

Thank you.

Respectfully,

_____

FOI Receiving Officer

ANNEX "F-6"

TEMPLATE - DOCUMENT NOT AVAILABLE

DATE

Dear_____,

Greetings!

Thank you for your request dated <insert data> under Executive Order No. 2 (s. 2016) on Freedom of Information in the Executive Branch.

Your request

You asked for <quote request exactly, unless it is too long/complicated>.

Response to your request

While our aim is to provide information whenever possible, in this instance this Office does not have [some ofl* the information you have requested. However, you may wish to contact <insert name of other authority/organization> at<insert contact details. Who may be able to help you. The reasons why we don't have the information are explained in the Annex to this letter.

Your right to request a review

If you are unhappy with this response to your FOI request, you may ask us to carry out an internal review of the response, by writing to <insert name of Chief, BJMP or RD, as the case may be, and postal / e-mail address>. Your review request should explain why you are dissatisfied with this response, and should be made within 15 calendar days from the date when you received this letter. We will complete the review and tell you the result, within 30 calendar days from the date when we receive your review request.

If you are not satisfied with result of the review, you then have the right to appeal to the BJMP Central Appeal and Review Committee pursuant to the BJMP FOI Manual.

Thank you.

Respectfully,

_____

FOI Receiving Officer

ANNEX "F-7"

TEMPLATE - UNDER EXCEPTIONS

DATE

Dear_____,

Greetings!

Thank you for your request dated <insert data> under Executive Order No. 2 (s. 2016) on Freedom of Information in the Executive Branch.

Your request
You asked for <quote request exactly, unless it is too long/complicated>.

Response to your request

While our aim is to provide information whenever possible, in this instance we are unable to provide [some of the information you have requested because an exception(s) under section(s) <insert specific section number(s) of the List of Exceptions applies to that information. The reasons why that exemption(s) applies are explained in the Annex to this letter.

Your right to request a review

If you are unhappy with this response to your FOI request, you may ask us to carry out an internal review of the response, by writing to <insert name of Secretary and postal / e-mail address>. Your review request should explain why you are dissatisfied with this response, and should be made within 15 calendar days from the date when you received this letter. We will complete the review and tell you the result, within 30 calendar days from the date when we receive your review request.

If you are not satisfied with result of the review, you then have the right to appeal to the BJMP Central Appeal and Review Committee pursuant to the BJMP FOI Manual.

Thank you.

Respectfully,

_____

FOI Receiving Officer