REPUBLIC OF THE PHILIPPINES
DEPARTMENT OF FINANCE
BUREAU OF INTERNAL REVENUE
Quezon City

JUN 0 9 2023

REVENUE MEMORANDUM CIRCULAR NO. 66-2023

SUBJECT: **Circularizing the Criminal Penalties for Violation of Provisions of Republic Act (RA) No. 10173 or the Data Privacy Act of 2012 and Administrative Penalties for Violation of Information and Communication Technology (ICT) Security Infrastructure System under Revenue Memorandum Order (RMO) No. 67-2010**

TO: **All Internal Revenue Employees, Officials and Others Concerned**

To afford full protection to a person's right to privacy and ensure that personal information and sensitive personal information are disclosed only as permitted under existing laws, this Circular is hereby issued to remind all revenuers that in case of unauthorized access, or leaks or premature disclosure of said information, the penalties provided under Chapter VIII of the Data Privacy Act of 2012 and Information and Communication Technology (ICT) Security Infrastructure Offenses, as implemented by Revenue Memorandum Order (RMO) No. 67-2010 shall be imposed.

I. PENALTIES UNDER THE DATA PRIVACY ACT OF 2012

OFFENSE	KIND OF INFORMATION AFFECTED	
	PERSONAL INFORMATION	SENSITIVE PERSONAL INFORMATION
Unauthorized Processing	**Imprisonment from 1 year to 3 years AND fine of not less than P500K to P2.0 Million**	**Imprisonment from 3 years to 6 years AND fine of not less than P500K to P4.0 Million**
Accessing Information Due to Negligence.		
Improper Disposal *(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).*	**Imprisonment from 6 months to 2 years AND fine of not less than P100K to 500K**	**Imprisonment from 1 year to 3 years AND fine of not less than P100K to P1.0 Million**

BUREAU OF INTERNAL REVENUE
RECEIVED
2:45 P.M.
JUN 09 2023
RECORDS MGT. DIVISION

OFFENSE	KIND OF INFORMATION AFFECTED	
	PERSONAL INFORMATION	SENSITIVE PERSONAL INFORMATION
Processing for Unauthorized Purposes	Imprisonment from 1 year 6 months to 5 years AND fine of not less than P500K to P1.0 Million	Imprisonment from 2 years to 7 years AND fine of not less than P500K to P2.0 Million
Unauthorized Access or Intentional Breach *(violating data confidentiality and security systems, breaking in any way into system storage)*	Imprisonment from 1 year to 3 years AND fine of not less than P500K to P2.0 Million	
Concealment of Security Breaches involving sensitive personal information	Imprisonment from 1 year 6 months to 5 years AND fine of not less than P100K to P1.0 Million	
Malicious Disclosure by PIP, PIC, or its agents, employees	Imprisonment from 1 year 6 months to 5 years AND fine of not less than P500K to P1.0 Million	
Unauthorized Disclosure	Imprisonment from 1 year to 3 years AND fine of not less than P500K to P1.0 Million	Imprisonment from 3 years to 5 years AND fine of not less than P500K to P2.0 Million
Combination or series of acts	Imprisonment from 3 years to 6 years AND fine of not less than P1.0 Million to P5.0 Million	

Note that 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. 35, RA 10173)

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. 36, RA 10173)

The penalties imposed are without prejudice to the filing of appropriate administrative case/s if the offender is a public official and employee.

II. PENALTIES FOR ICT SECURITY INFRASTRUCTURE OFFENSES UNDER REVENUE MEMORANDUM ORDER (RMO) NO. 67-2010

ACTS COMMITTED	OFFENSE	PENALTY
◦ Disclosure of sensitive information without management approval ◦ Unsecured Super User and other powerful accounts ◦ Disclosure of user ID and password without consent ◦ Failure to disclose to proper authorities any event or incident of violations and/or security breaches discovered by and/or made known to him/her ◦ Other Analogous cases	**Gross Neglect Of Duty**	**Dismissal from service on the first offense**
◦ Unauthorized user access to BIR Offices ◦ Unauthorized access to operating system ◦ Unauthorized access to database ◦ Unauthorized alterations to system objects and files ◦ Unauthorized access to the network ◦ Unauthorized access to application systems ◦ Unauthorized access to machines (PCs, servers, peripherals, etc., holding or transmitting applications or data) ◦ Unauthorized copying of BIR software and data ◦ Installation of unauthorized software ◦ Unauthorized access to external storage media (flash drives, optical media, etc.)	**Grave Misconduct**	**Dismissal from service on the first offense**
• Unauthorized users gaining access to the system via logged-in workstations • Adding an unauthorized PC or other devices to the network ◦ Disclosure of user ID and password even with his/her consent • Misrepresentation or falsification of his/her identity on the internet or in any BIR system or communications ◦ Disruption of the operations of the BIR's information and communication technology systems ◦ Unauthorized disabling of hardware, software, monitoring tool installed on any system or network		

ACTS COMMITTED	OFFENSE	PENALTY
◦ Abuse of access privileges ◦ Unauthorized download, installation, storage or transmittal of software not licensed to the BIR ◦ Unauthorized probing or cracking of security mechanisms either at BIR or external sites ◦ Unauthorized establishment of internet or other external network connections ◦ Unauthorized setting-up of proxy servers ◦ Other analogous cases		
◦ Unauthorized alterations (addition, modification, deletion) to printouts (reports, correspondences, etc.) and electronic files ◦ Other analogous cases	**Falsification of official documents**	**Dismissal from service on the first offense**

III. ADDITIONAL CIRCUMSTANCES AS GROUNDS FOR ADMINISTRATIVE DISCIPLINARY ACTION WITH THEIR CORRESPONDING PENALTIES UNDER RMO NO. 67-2010

ACTS COMMITTED	OFFENSE	PENALTY
◦ Disclosure of sensitive information without priormanagement approval • Unsecured superuser and other powerful accounts ◦ Disclosure of user id and password without consent • Failure to disclose to proper authorities any event or incident of violations and/or security breaches discovered by and/or made known to him/her • Other analogous cases	**Grave Misconduct**	**Dismissal from service on the first offense**

ACTS COMMITTED	OFFENSE	PENALTY
◦ Unauthorized user access to BIR offices ◦ Unauthorized access to the operating system ◦ Unauthorized access to the database • Unauthorized alterations (addition, modification, deletion) to system objects and files, application, data and logs ◦ Unauthorized access to the network • Unauthorized access to application systems ◦ Unauthorized access to machines (PCs, servers, peripherals, etc.) holding or transmitting applications or data ◦ Unauthorized access to printed output (reports, correspondences, etc.) and electronic files • Unauthorized copying of BIR software and data ◦ Installation of unauthorized software • Unauthorized access to external storage media (tape cartridges, flash drives, optical media, floppy disks, etc.) • Unauthorized users gaining access to the system via logged-in workstations • Adding an unauthorized PC or other devices to the network • Disclosure of user id and password even with his/her consent ◦ Misrepresentation or falsification of his/her identity on the internet or in any BIR system or communications ◦ Disruption of the operations of the BIR's information and communication technology systems	**Gross Neglect Of Duty**	**Dismissal from service on the first offense**
• Unauthorized disabling of hardware, software, monitoring tool installed on any system or network ◦ Abuse of access privileges • Unauthorized download, installation, storage or transmittal of software not licensed to the BIR ◦ Unauthorized probing or cracking of security mechanisms either at BIR or external sites • Unauthorized establishment of internet or other external network connections ◦ Unauthorized setting-up of proxy servers		

ACTS COMMITTED	OFFENSE	PENALTY
∘ Unauthorized alterations (addition, modification, deletion) to printouts (reports, correspondences, etc.) and electronic files ∘ Other analogous cases	**Falsification of official documents**	**Dismissal from service on the first offense**

For your strict compliance.

ROMEO D. LUMAGUI, JR.
Commissioner of Internal Revenue
009336

L/

BUREAU OF INTERNAL REVENUE
RECEIVED
2:45 pm
JUN 09 2023
RECORDS MGT. DIVISION