(Translation)

Personal Data Protection Policy for Employees

Personal Data Protection Policy for Employees
of Amarin Corporations Public Company Limited and Its Affiliates

---

1. General Principles

1.1 Introduction

Amarin Corporation Public Company Limited and its affiliates ("Company") realize the importance in protecting Personal Data of all employees. We have a commitment to comply with the Personal Data Protection Law. As a result, we have developed a personal data management system with advanced operating systems and information technology to ensure effective security in Personal Data protection. We also provide a system to strictly monitor the access and the use of Personal Data and consistently improve and develop personal data storage systems to promote validity and reliability of the storage system in order to prevent leak of Personal Data, modification to Personal Data without relevant staff, or use of Personal Data for any purpose other than those notified by the Company to the relevant persons.

This document outlines types of Personal Data and purposes of the collection, use, or disclosure of Personal Data, retention period of Personal Data, types of persons or entity to whom the collected Personal Data may be disclosed by the Company, data subject rights, security measures on Personal Data in compliance with the provisions of law, as well as other information relevant to the Personal Data management of the Company.

This document is a company policy. All and any notices, rules, or regulations in contrary or not in accordance with this document shall be substituted by clauses in this document from the date this document becomes effective.

This document is also considered a part of the Terms and Conditions of Use or Terms of Service of the Company. The Company may modify, change, add, or alter this Policy by giving you a notice and requesting a consent from you as required by the law related to personal data protection.

1.2 Definitions

To enable clear communication with any relevant person and create no concern about interpretation of certain terms herein, the Company provides definitions as follows.

"**Company**" means Amarin Corporations Public Company Limited and its Affiliates, including a person or persons authorized to act on behalf of Amarin Corporations Public Company Limited and its Affiliates.

"**Affiliates**" mean Amarin Book Center Co., Ltd., Dek-D Interactive Co., Ltd., Amarin Television Co., Ltd., Amarin Omniverse Co., Ltd., AME Imaginative Co., Ltd, as well as any other companies of which issued

shares are held by the Company in total of 50 percent or more (first-tier subsidiaries) and other companies of which shares are held by the first-tier subsidiaries and/or subsidiaries at any subsequent tier in total of 50 percent and more. This also includes the definition of the term "Affiliates" according to regulations currently provided or to be amended in the future by regulatory authorities.

"**Personal Data Protection Law**" means the Personal Data Protection Act, B.E. 2562 (2019) or other amended versions, including royal decrees, ministerial regulations, notices, orders, and other legislations in relation to personal data protection.

"**Personal Data**" means data relating to natural person which is identifiable to that person either directly or indirectly.

"**Processing**" means collection, use or disclosure of Personal Data.

"**Personal Data Controller**" means a person or legal entity with authority to make decisions on colleting, using, or disclosing Personal Data.

"**Personal Data Processor**" means a person or legal entity who performs collection, use, or disclosure of Personal Data according to the commands, or on behalf, of the Personal Data Controller, provided that such person or legal entity is not a Personal Data Controller.

"**Personal Data Subject**" means a natural person, director, representative of a legal entity, as well as representative of the aforementioned persons who receive any form of service from the Company.

1.3 Concernment

The Company shall consider carefully to collect, use, disclose Personal Data of a relevant person under the objectives of business operations according to the law by the following grounds.

1.3.1 It is in accordance with the provisions of law.

1.3.2 It is necessary for fulfilling business contracts to which the Personal Data Subject is a counterparty with the Company.

1.3.3 It is necessary other than those provided by laws, or to fulfill contracts, or to offer a welfare or benefits to the Personal Data Subjects in a higher degree than a general counterparty.

2. The Principles of Limited Data Collection

2.1 Personal Data to Be Collected

This Policy shall apply to the following Personal Data that the Company may collect, including the cases where the Personal Data Subject has given consent to the Company.

(a) General Personal Data: data identifiable to the Personal Data Subject, either directly or indirectly, as follows.

- Employee contact information, e.g., name-surname, nickname, address, emergency contact person, telephone number, email, social media account
- Employee identity information, e.g., date of birth, gender, photo or video, marital status, military status
- Information of family members or people under custody of employees, e.g., information of spouses, children, beneficiaries, work guarantor, etc.
- Employees' documents of identity and vehicle, e.g., copy of ID card, copy of driver's license, copy of other documents issued by government agencies, copy of car or motorcycle registration
- Information on education, abilities, skill development, and other qualifications of employees, e.g., copy of the license for professional practice, copy of training certificate, copy of graduation certificates, education background, training experience, language abilities, and other abilities provided by employees to the Company
- Work information, e.g., position, work performance, and work history
- Financial information, e.g., bank account information, wage, salary, income, tax, tax deduction or exemption, provident fund, credit union, funeral welfare, loan
- Information relating to social securities, labor protection, employees' benefits and welfares under the regulations on human resource management of the Company, and other information that is necessary for fulfilling the employment contract, management of the benefits and welfares of employees and the operation of the Company
- Information on the work entry-exit records, working period, overtime, absence, and leave
- Information on the participation in events of the Company, including information disclosed by the employee to the Company through the systems or applications of the Company, e.g., participating in events, responding to registration forms or surveys, interviews
- Data on complaints, whistleblowing, investigation, disciplinary punishments
- Identifiable information of devices or tools, such as IP Address, Cookie ID; access history to websites, applications, or programs of the Company; types of browsers used for access.
- Any other information that is deemed to be Personal Data under the Personal Data Protection Law.

(b) Sensitive Personal Data: any personal data categorized as sensitive personal data under Section 26 of the Personal Data Protection Act, B.E. 2562 (2019). Examples are as follows:

- Health information, e. g. , weight, height, congenital disease, blood group, data of physical disability, health information, medical examination results, medical treatment records, occupational or non-occupational hazard incident records that are presented to the Company, disease diagnostic results, prescription record, medication record, medical treatment receipt of payment, drug abuses
- Data regarding ethnicity, nationality, race, doctrine belief, religion, labor union information, sexual behavior, criminal record
- Biometric data, e.g., scanning images of face, eyes, fingerprint, as well as genetic data
- Any other necessary data that is subject to explicit consent of the Employee or in accordance with other purposes provided by law.

2.2 Collection of Personal Data

2.2.1 General Personal Data

Although the Company will be able to collect Personal Data of a relevant person as direct a counterpart, or a representative of a legal entity, or an authorized assignee to perform any legal act as a counterparty, without obtaining consent according to the principle of consent under the laws, the Company also continues to maintain participations by providing the relevant person with an explicit notice that the counterparty shall need to provide only Personal Data to the extent necessary for entering into contracts as a counterparty while the Company and that the relevant person must comply with the laws in connection with such legal acts or contracts. Apart from those stipulated, the Company may collect data without obtaining consent from Personal Data Subject in the following cases:

(a) It is to fulfill the research or statistic purpose, provided that appropriate measures are in place to protect the rights and liberty of the Personal Data Subject, in compliance with provisions of law.

(b) It is to prevent or restrain harm to one's life, body, and health.

(c) It is necessary to fulfill the contract to which the Personal Data Subject is a counterpart to the Company or to be used for proceeding with requests of the Personal Data Subject before entering into any contract with the Company.

(d) It is necessary to perform duties on the Company's missions for public interests, or to perform duties in exercising the state power granted to the Company.

(e) It is necessary for the legitimate interests of the Company or other natural persons or legal entities that are not the Company, unless such interests are less important than fundamental rights in Personal Data of the Personal Data Subject.

(f) It is to comply with the laws by the Company.

2.2.2 Sensitive Personal Data

The Company may collect sensitive Personal Data without asking for consent from Personal Data Subject in the following cases.

(a) It is necessary for the Company to proceed with the collection in order to prevent or restrain harm to one's life, body, and health, while the Personal Data Subject is unable to give consent for any reason.

(b) It is the data of the Personal Data Subject who has already given explicit consent to any other Personal Data Controllers to disclose it to the public.

(c) It is necessary for the Company to enable establishment of the legal rights of claim, compliance, or exercise of the legal rights of claim, or defense against the legal rights of claim.

(d) It is necessary for the Company to proceed with the collection in order to comply with the law to accomplish the objectives on preventive medicine or occupational medicine, assessment on employees' working ability, medical disease diagnosis, or for public interests on public health, as well as to comply with the laws on labor protection, social security, national health security, medical treatment welfares, car insurance coverage, social protection, statistical research, or other public interests, including any actions for significant public interests, provided that appropriate measures are provided by the Company to protect fundamental rights and benefits of the Personal Data Subject.

2.2.3 Personal Data of Minors, Incompetent Persons, and Quasi-incompetent Persons

The Company will process Personal Data of minors, incompetent persons, and quasi-incompetent persons only when obtaining consent from the guardians with authority to act on behalf of minors, custodians, or curators (as the case may be), except for the case that such person is allowed by laws to give consent solely by him/herself.

In the event that the Company has not obtained consent from a person with authority to give consent on behalf of minors, incompetent persons, or quasi-incompetent persons and does not know at the time of processing the Personal Data that the Personal Data Subject is a minor, incompetent person, or quasi-incompetent person, the Company shall delete or destroy or make the Personal Data of the Personal Data Subject unidentifiable to such person, except for the case that the Company is allowed to process the Personal Data of such person by laws without asking for consent.

3. Purposes of the Collection, Use, and/or Disclosure of Personal Data

Personal Data of an employee shall be collected, used, or disclosed by the Company for legitimate purposes as follows.

(a) To comply with laws, regulations, or orders of legal authorities, such as labor protection law, labor relations law, social securities law, the law on work safety, occupational health, and environment, communicable disease control law, etc.

(b) For legitimate interests of the Company, e.g. to be used for conducting a database of employees of the Company for human resources management, manpower analysis and allocation, personnel development, the provision of medical treatment welfare and other welfares; to be used for executing and sending the data to external agencies as part of the compliance with the laws relating to labor protection, including the office of social security fund, medical treatment facilities, insurance companies, the office of provident fund, the revenue office, medical welfares for employees' family members, the Department of Skill Development, the Legal Execution Department, the Student Load Fund Office, loans from commercial banks, the Department of Agriculture, the Department of Business Development, the Department of Intellectual Property, the Office of Consumer Protection Board, the Electronic Transaction Development Agency of the Ministry of Digital Economy and Society, and any agencies provided by laws or based on the application of the employee; to be used for office management, internal contact and coordination, execution on loan or suretyship contracts for employees, expense disbursement, asset possession, building and facilities management, letters and posts handling, workplace entry-exit record, inspection and assessment by internal and external agencies; to send, transfer, or disclose to delivery service providers as part for contacting customers; to transmit the data to banks for proceeding with payouts of salary, renumeration, reward, bonus, and welfare.

(c) To proceed with the request of employees before entering into contracts or to fulfill the contracts; the Company shall process the Personal Data of an employee to the extent provided in the employment contract made by and between the Company and the employee, e.g. verifying the identity to enter the work or access the internal information system, calculating and paying wages and returns, evaluating work performance, allocating position and duties to match health conditions of employees, adjusting wages; to collect data on the past disciplinary behaviors and penalties, criminal records; to provide trainings; to manage human resources as employees of the Company according to the employment contract, including work promotion and transfer, disbursement according to the work regulations, transport ticket reservation, visa application, reservation for accommodations and hospitalities, medical health checkup as

required by law and as provided by the Company; as well as to provide welfares and benefits to employees and their family.

(d) To prevent and restrain harm to one's life, body, and health; to be used for contacting the employee or relevant person in any emergency case or for employees' health and safety management. Regarding family members of the employee, the Company shall process their Personal Data on a necessity basis for benefits of emergency cases.

(e) To fulfill the purposes according to the consent given by the employee.

4. The Principles of Personal Data Security

4.1 Manual Storage of Personal Data

Documents shall be filed and stored in locked filing cabinets and/or in locked rooms. Only staff can access the data.

4.2 Storage of Personal Data in Electronic Systems

The Company has provided security measures of Personal Data by considering the fundamental rights of relevant individuals by designing the information systems, networking systems, and computers that optimize security and support the operations of the Company to be corresponding to the provisions of applicable laws and prevent threats that can cause damage to the Company as follows.

4.2.1 Policies on information technology security are provided in writing and communicating the policy to raise understanding and follow in the right way, especially among those in the information technology department and other departments within the company to coordinate and operate the business to achieve the set goals.

4.2.2 Reviews of the policy on information technology security shall be carried out at least once a year or when there is any change that affects information technology security of the Company.

4.2.3 A specific person is assigned with duties and responsibilities for information technology risk management to ensure that the Company can provide information technology approaches or guidelines to mitigate or handle the existing risks and propose it to executives to consider information technology risk management.

4.2.4 The risks relating to information technology are identified, covering significant risks such as risks arising from personnel, software and data from network systems and internet, hardware and computer devices, financial risks, and risks of flood, storm, fire, earthquake, building collapse, theft, and power outage

4.2.5 Satisfactory approaches to manage and handle risks are defined, conducting a table clarifying features and descriptions of risks including title, name of risks, type of risks, characteristic of risks, risk factors, and effects, etc. and the possibility of occurrence and severity level of risk effects must be identified.

4.2.6 Personnel of the Company are not allowed to use computer networks for committing illegal acts or acts contrary to public order and good morals, such as the provision of websites for trading or publicizing things that are illegal or contrary to good morals.

4.2.7 Use of computer networks or computer devices with usernames of others, either permitted or not permitted by the username owner, is not allowed.

4.2.8 Access to computer systems and information of others that are prevented from unauthorized access in order to edit, delete, add, or copy is prohibited.

4.2.9 It is prohibited to disseminate information of others or agencies without authorization by the owner of such information.

4.2.10 No one is allowed to disturb, hinder, or damage resources and computer networks of the Company, e.g., sending computer viruses, entering programs that disable the operation of computers or networking devices.

4.2.11 No one is allowed to smuggle trapping information in the computer networks of the Company and others who are in the process of information transmission within the computer networks.

4.2.12 Users are required to scan viruses with an anti-virus program every time before using portable media or opening files attached to emails or files downloaded from the internet.

4.2.13 Users in the IT Department are assigned to keep the information system of the Company secured, and control the operation of the system to maintain the policies and practices of the Company on the security of information systems.

4.2.14 All employees of the Company must be responsible for complying with the policies and guidelines of the Company regarding security of information systems and must not commit any breach of the law on computer-related offense.

4.2.15 Users are not allowed to install, modify, or change any program in computers of the Company, unless advised by administrator or permitted by the top authority of any agencies.

4.2.16 Network connection routes shall be provided for accessing the internet system with security systems such as Firewall. Before connecting to the network system, computers of the Company shall be installed with ant-virus programs, and the vulnerability of the operating system shall be resolved. After

completing the use of the internet system, users are required to close the web browser to prevent access by third parties.

4.2.17 Users shall access information according to their rights based on their duties and responsibilities for the effectiveness of the network systems and the security of the Company. Users are prohibited from disclosing important data which the Company keeps confident, unless it is in accordance with the official rules of disclosure of the Company.

4.2.18 To categorize levels of confidentiality, data shall be classified into types based on its function and priority of data. Each type of data shall be determined with how to manage and how to handle confidential data or prioritized data before terminating or reusing it. Transmission of important data through public networks must be subject to global standard encryption, such as Secure Socket Layer, Virtual Private Network (VPN), etc.

4.2.19 Measures to control the validity of the stored, imported, processed, and displayed data shall be in place. In case the data is stored in many places or related data sets are collected, the data must be controlled to have the same validity. This includes measures on data security in the event that computer devices are taken out of the Company area, e.g. for repair. Also, data stored in any saving materials shall be destroyed.

4.2.20 control of access to information and devices for processing data with consideration for usage and the security on the use of information systems. Rules for access authorization and user rights shall be determined for users at all levels to acknowledge, understand, and practice according to the rules, and realize the importance of the security of the information systems. The rights to use the information and information system, including the right to use programs and information systems, the right to access the internet, etc., shall be determined to users in accordance with their duties and responsibilities. The rights will be given as necessary for the operation of their duties and must be approved by an authorized person in writing and shall be reviewed regularly.

4.2.21 In case that the user, as a Personal Data Subject, is necessary to give others the right to access or modify any of his/her important Personal Data, e.g., file shares, the right must be given to specific individuals or specific groups of people and must be terminated if it becomes unnecessary and the Personal Data Subject needs to have proof of the grant of the right and specify a period of use and suspend the use immediately when the period is over.

4.2.22 In case of necessity to give others the rights to access an information system and networking system in a temporary and urgent manner, it must be proceeded according to procedures and

practices as well as approved by the authorized person every time. Reasons and needs must be noted including duration for the use. The access shall be suspended immediately when the duration is over.

4.2.23 Authentication and license verification systems are provided. Users are required to log in to the system with a strong and unpredictable password. Each user shall be provided with an individual account. However, determining whether the password is strong and unpredictable or not is under the control of the Company according to its rules and regulations.

4.2.24 Users are required to verify their identity before accessing the system with a password assigned by the administrator. The password should be changed regularly. Each time you change it should not be identical to the last 3 passwords you previously changed and kept confidential, not noting it on paper and attaching the paper on the screen. In the case of shared users, the administrator shall notify the users to change the password when there is a change of any affiliated users.

4.2.25 A system for regularly checking names of the users of key systems is provided. The name list of the users with unauthorized access to systems will be reviewed, e.g. the name list of resigned employees, the name list associated with the systems and the use of the systems shall be suspended immediately when detecting unauthorized access by disabling or removing from the system or changing passwords.

4.2.26 A Data Center Room is provided proportionally, including the networking system section, computers and hosts section, uninterruptable power supply section, battery and power supply section, for convenience in the operation and to control the access to key computers more effectively.

4.2.27 Agreements on data transfer shall be provided with consideration on security of the data and system administrator must control the operation to be secure in 3 aspects: Confidentiality, Integrity, and Availability. A contract between the Company and any third-party agency shall be made and signed to ensure that confidential information of the Company shall not be disclosed. Also, measures for monitoring and inspecting the operation and the quality of the service provision of third-party providers shall be in place to ensure compliance with the contracts and agreements.

5. The Principles of Disclosure

The Company may disclose Personal Data of employees and any relevant person as mentioned above to any person or legal entity as follows.

5.1 Government agencies of which notices, rules, and provisions must be complied by the Company, including the Revenue Department, the Social Security Office, the Department of Business Development, the Office of Consumer Protection Board, Thai Industrial Standard Institute, the Securities and Exchange

Commission, the Customs Department, the Department of Employment, the Department of Labor Protection and Welfare, the Department of Skill Development, the Department of Lands, the Department of Provincial Administration, etc.

5.2 Partners: the Company may disclose your Personal Data to others who have entered into an agreement as partners with the Company, such as financial institutions, insurance companies, healthcare facilities, securities companies, fund management companies, for benefits of relevant persons.

5.3 Professional Service Providers, including financial consultants, legal counselors, quality system consultants, auditors, internal auditors

5.4 Infrastructure and information technology providers, data storage providers, and Cloud service providers

5.5 Marketing, statistics, advertising, public relations, and communication service providers

5.6 Any other people as required by law: In case the Company is required by applicable laws, regulations, rules, orders of government or regulatory agencies, or orders of judicial authority, to disclose your Personal Data

5.7 Assignees of the rights and/or duties from the Company: In case the Company wishes to assign its rights and duties, including entire or partial business transfer, merger, and shareholding reconstruction, the Company needs to disclose your Personal Data to the assignees (including potential assignees); whereas, the rights and duties of the assignees in respect to your Personal Data shall be subject to this Policy.

6. Transmission or Transfer of Personal Data to Foreign Country

The Company may be required to send or transfer your Personal Data to a foreign country. The Company shall carry out appropriate procedures for protecting personal data security at the same level as the Personal Data Protection Law of Thailand.

7. Cookies

The Company may use Cookies and similar technology when you access the websites, applications, or electronic materials of the Company. For more information, please refer to Cookies Policy.

8. Personal Data Subject's Rights

8.1 Right to be informed. Personal Data Subjects has the right to be informed how his/her Personal Data is collected, used, or disclosed either before or at the time the Company collects his/her Personal Data, which the Company has primarily informed Personal Data Subject through this Policy.

8.2 Right to access, request for copies, or to be disclosed how Personal Data is obtained. Personal Data Subject has the right to request access or copies of his/her Personal Data. Also, Personal Data Subject

can ask the Company to disclose how his/her Personal Data was obtained if the Personal Data did not give consent for collecting such Personal Data. The Company reserves the right to charge an operation cost for retrieving your saved Personal Data, and the Company will notify you of the operation cost before executing your request.

8.3 Right to object. Personal Data Subject has the right to object to the collection, use, and disclosure of Personal Data relating to the Personal Data Subject if the data is collected without obtaining his/her consent, or the data is collected, used, or disclosed for a purpose of direct marketing or research.

8.4 Right to erasure, destruction, and restriction. Personal Data Subject has the right to request the Company to delete, destruct, or restrict the use of his/her Personal Data stored by the Company, or to make the Personal Data unidentifiable to him/her if the Personal Data Subject revokes or objects to the collection, use, or disclosure of Personal Data relating to him/her, or when it is no longer necessary to collect, use, or disclose it according to the purposes as he/she gave consent for, or when the Company commits a breach to the Personal Data Protection Law.

8.5 Right to rectification. Personal Data Subject has the right to request the Company to rectify his/her Personal Data stored by the Company to be correct, up-to-date, complete, and non-misleading.

8.6 Right to withdraw consent. Personal Data Subject has the right to withdraw consent for the collection, use, and disclosure of his/her Personal Data. However, the withdrawal shall not affect the collection, use, or disclosure of the Personal Data that he/she has already given consent for. The withdrawal of consent may cause the Company to no longer provide services to you.

8.7 Right to data portability. Personal Data Subject has the right to request the Company to send your Personal Data to you or another Personal Data Controller if the data is in a transferable format.

8.8 Right to file a complaint. Personal Data Subject has the right to file a complaint to authority agencies if the processing to his/her Personal Data is not in compliance with the Personal Data Protection Law.

To exercise the rights, you, as a Personal Data Subject, acknowledge that your rights specified herein are limited under the applicable laws and that the Company may refuse your exercise of rights if the Company has a legitimate reason to do so.

However, exercising the rights as a Personal Data Subject hereunder shall be limited only to basic services that cause no unnecessarily excessive expenses to Personal Data Controller. If the exercise of the Personal Data Subject' s rights by any relevant person causes damages, fees, or expenses for the execution

on the request of the Personal Data Subject, the Personal Data Subject shall be liable for compensating or repaying the cost for the execution of such requests.

9. The Principles of Responsibility

9.1 Personal Data Retention Period

Unless otherwise specified by law, the Company shall retain your Personal Data for a period as necessary for completing the purposes of processing the Personal Data as specified herein or until the Company is notified of a withdrawal of consent for collecting the Personal Data by the Personal Data Subject.

9.2 Deletion and Destruction Monitoring System for Personal Data When the Retention Period Is Over

The Company provides a deletion and destruction monitoring system for Personal Data of relevant persons when the retention period is over, or it exceeds the necessity according to the purposes or as requested by the Personal Data Subject, or when the Personal Data Subject withdraws his/her consent, except for the case where the Company is required to retain it for purposes of exercising its freedom of expression, or it is under the exemptions of the laws specifically stipulated, establishing the legitimate rights of claim, fulfilling the exercise of legitimate rights of claim, defending against the exercise of legitimate rights of claim, or complying with laws.

9.3 Third-party Websites or Service Providers

Websites, services, or platforms of the Company may include links to websites, services, or platforms operated by any third parties, such as service fee payment providers. The Company shall not be responsible for securing the privacy of the websites operated by such third parties. Therefore, the Company suggests you review the personal data protection policy of the websites or services operated by third parties to consider how the Personal Data collected from you is handled.

9.4 Details of the Company as the Personal Data Controller

If you want to contact the Company to exercise the rights on your Personal Data, or if you have any inquiry about your Personal Data, please contact the Company with the following information:

Personal Data Controller

Amarin Corporation Public Company Limited and Its Affiliates

Head Office: 378 Chaiyapruek Road, Taling Chan Subdistrict, Taling Chan District, Bangkok 10170

Tel.: 02-422-9999

The Office of Personal Data Protection

Email: dpooffice@amarin.co.th

Personal Data Subject and/or relevant person can refer to the Personal Data Protection Policy of the Company at www.amarin.co.th.

10. Penalty on the Failure to Comply with the Personal Data Protection Policy

Failures to comply with the Personal Data Protection Policy of the Company can be considered offenses that result in disciplinary penalties and legal punishment.

11. Change to the Personal Data Protection Policy of the Company

The Company may amend this announcement from time to time to be consistent with the Personal Data Protection Law and shall notify you of the change via the website or other communication channels of the Company.

This Personal Data Protection Policy shall be effective on January 1st, 2026, henceforth.

Declared on December 4th, 2025