DATA PROTECTION POLICY

Applies to all processing of personal data of natural persons.

1 PURPOSE, SCOPE AND USERS

As part of its social responsibility, Inkron (the "Company") is committed to compliance with data protection laws such as the General Data Protection Rule ("GDPR"). This Data Protection Policy applies worldwide to the Company and sets out our commitment to data protection and our obligations in relation to personal data, as well as our commitment towards individual rights.

2 REFERENCED DOCUMENTS / MANUALS / STANDARDS

General Data Protection Regulation EU GDPR 2016/679

3 DEFINITIONS

"personal data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

"Sensitive Personal Data" Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Those personal data include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation

"processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

"restriction of processing" means the marking of stored personal data with the aim of limiting their processing in the future

"processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

"recipient" means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing

"third party" means a natural or legal person, public authority, agency or body other than the data subject, Company, processor and persons who, under the direct authority of the Company or processor, are authorized to process personal data

"consent" of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her

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

"representative" means a natural or legal person established in the Union who, designated by the Company or processor in writing, represents the Company or processor with regard to their respective obligations under the GDPR;

"group of undertakings" means a controlling undertaking and its controlled undertakings;
12. "supervisory authority" means an independent public authority which is established by a Member State pursuant to Article 51of GDPR;

"international organisation" means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

"Commission" means the European Commission.

"Union" means the European Union.

"Member States" means member states of the European Union.

"EEA" means the European Economic Area, i.e. the economic region associated with the EU including Norway, Iceland and Liechtenstein.

4 PRINCIBLES RELATING TO PROCESSING OF PERSONAL DATA

4.1 LAWFULNESS, FAIRNESS AND TRANSPARENCY

Personal data must be collected and processed in a lawful, fair and transparent manner in relation to the data subject.

4.2 PURPOSE LIMITATION

Personal data must only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

4.3 TRANSPARENT INFORMATION

The data subject must be informed of how his/her data is being handled. In general, personal data must be collected directly from the individual concerned. When the data is collected, the data subject must be either be aware of, or informed of, the following information to ensure fair and transparent processing, depending on the situation:

- ✓ The identity and the contact details of the Company and its representative
- ✓ The purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- ✓ The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period
- ✓ The existence of the right to request from the Company access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability
- ✓ The existence of the right to withdraw any given consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal
- ✓ The right to lodge a complaint with a supervisory authority

4.4 DATA MINIMIZATION AND DELETION

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. Personal data that is no longer needed for the purposes for which they were initially collected must be deleted.

4.5 STORAGE LIMITATION

Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

4.6 ACCURACY

Personal data on file must be correct, complete, and kept up to date.

4.7 INTEGRITY AND CONFIDENTIALITY

Personal data must be processed in a manner that ensures appropriate security of the personal data. This includes the use of technical or organizational measures to protect the data against unauthorized or unlawful processing and against accidental loss, destruction, or damage.

5 BASIS OF DATA PROCESSING

Collecting, processing and using personal data is permitted only under the following legal bases.

5.1 CUSTOMER AND PARTNER DATA

5.1.1 DATA PROCESSING FOR A CONTRACTUAL RELATIONSHIP

Personal data of the relevant prospects, customers and vendors can be processed in order to prepare, execute and terminate a contract. This also includes advisory services for the customers or vendors under the contract if this is related to the contractual purpose. Prior to a contract – during the contract initiation phase – personal data can be processed to prepare bids or purchase orders or to fulfill other requests of the prospect that relate to contract conclusion.

5.1.2 DATA PROCESSING FOR ADVERTICING PURPOSES

If the data subject contacts the Company to request information (e.g. request to receive information material about a product), data processing to meet this request is permitted.

Personal data can be processed for advertising purposes or market and opinion research, as long as this is consistent with the purpose for which the data was originally collected.

Data subjects have a right to object to processing for advertising purposes. Once the data subject objects to or refuses the use of his/her data for advertising purposes, it can no longer be used for these purposes and must be blocked from use for these purposes.

5.1.3 PROCESSING THE SPECIAL CATEGORIES OF DATA

Special categories of data is data about racial and ethnic origin, political opinions, religious or philosophical beliefs, union membership, genetic or biometric data, data concerning health and data concerning a natural person's sex life. Special categories of data can generally only be processed if the data subject has given his/her express consent.

5.2 EMPLOYEE DATA

5.2.1 DATA PROCESSING FOR THE EMPLOYEMENT RELATINSHIP

In employment relationships, personal data can be processed if needed to initiate, carry out and terminate the employment agreement. When initiating an employment relationship, the applicants' personal data can be processed.

In the existing employment relationship, data processing must always relate to the purpose of the employment agreement if none of the following circumstances for authorized data processing apply.
If it should be necessary during the application procedure to collect information on an applicant from a third party, the requirements of the corresponding national and international laws have to be observed. In cases of doubt, consent must be obtained from the data subject.

5.2.2 COLLECTIVE AGREEMENTS ON DATA PROCESSING

If a data processing activity exceeds the purposes of fulfilling a contract, it may be permissible if authorized through a collective agreement. Collective agreements are pay scale agreements or agreements between employers and employee

representatives, within the scope allowed under the relevant employment law. The agreements must cover the specific purpose of the intended data processing activity and must be drawn up within the parameters of national data protection legislation.

5.2.3 DATA PROCESSING TO LEGITIMATE INTEREST

Personal data can also be processed if it is necessary to enforce a legitimate interest of the Company. Legitimate interests are generally of a legal (e.g. filing, enforcing or defending against legal claims) or financial (e.g. valuation of companies) nature. Personal data may not be processed based on a legitimate interest if, in individual cases, there is evidence that the interests of the employee merit protection.

Control measures that require processing of employee data can be taken only if there is a legal obligation to do so or if there is a legitimate reason.

5.2.4 PROCESSING OF SPECIAL CATEGORIES OF DATA

Special category personal data can be processed only under certain conditions. Special categories of data is data about racial and ethnic origin, political opinions, religious or philosophical beliefs, union membership, genetic or biometric data, data concerning health and data concerning a natural person's sex life. Under national law, further data categories can be considered as special categories of data or the content of the data categories can be filled out differently. Moreover, data that relates to a crime can often be processed only under special requirements under national law.

Special categories of data can generally only be processed if the data subject has given his/her express consent.

6 DATA TRANSFER

Personal data must not be transferred to outside the EEA, except when the Company transfers personal data to NAGASE & CO., LTD. in Japan or other NAGASE group companies pursuant to the Standard Contractual Clauses concluded between the Company and the respective recipient.

7 CONFIDENTIALITY PROCESSING

Personal data is subject to data secrecy. Any unauthorized or unlawful processing, access or destruction by employees is prohibited. Any data processing undertaken by an employee that he/she has not been authorized to carry out as part of his/her legitimate duties is unauthorized. Employees may have access to personal information only as is appropriate for the type and scope of the task in question. This requires a careful breakdown and separation, as well as implementation, of roles and responsibilities.

Employees are forbidden to use personal data for private or commercial purposes, to disclose it to unauthorized persons, or to make it available in any other way. Supervisors must inform their employees at the start of the employment relationship about the obligation to protect data secrecy. This obligation shall remain in force even after employment has ended.

8 RIGHTS OF INDIVIDUAL DATA SUBJECTS

8.1 RIGHT OF ACCESS

The data subjects have the right to obtain from the Company the confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

- ✓ The purposes of the processing
- ✓ The categories of personal data concerned
- ✓ The recipients or categories of recipient to whom the personal data have been or will be disclosed
- ✓ Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period

- ✓ The existence of the right to request from the Company rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing
- ✓ The right to lodge a complaint with a supervisory authority

If requested, the Company must give the data subject a copy of the personal data undergoing processing. For any further copies requested by the data subject, the Company may charge a reasonable fee based on administrative costs.

8.2 RIGHT TO RECTIFICATION

The data subjects have the right to obtain from the Company without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subjects have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

8.3 RIGHT TO ERASURE

The data subjects have the right to obtain from the Company the erasure of personal data concerning him or her without undue delay, on the condition that one of the following grounds applies:

- ✓ The personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed
- ✓ The data subject withdraws consent on which the processing is based, and where there is no other legal ground for the processing
- ✓ The personal data have been unlawfully processed
- ✓ The personal data must be erased for compliance with a legal obligation in Union or Member State law to which the Company is subject

However, the preceding paragraph of this Section 3 of Article VII shall not apply to the extent that processing is necessary:

- ✓ For exercising the right of freedom of expression and information
- ✓ For compliance with a legal obligation which requires processing by Union or Member State law to which the Company is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Company
- ✓ For reasons of public interest in the area of public health
- ✓ For the establishment, exercise or defense of legal claims.

8.4 RIGHT TO DATA PORTABILITY

The data subjects have the right to receive the personal data concerning him or her, which he or she has provided to the Company, in a structured, commonly used and machine-readable format, and have the right to transmit those data to another controller without hindrance from the Company.

9 RECORDS OF PROCESSING ATIVITIES

The Company must maintain a record of processing activities. That record must contain the following information:

- ✓ The name and contact details of the Company and, where applicable, the joint controller, the Company's representative and the data protection officer
- ✓ The purposes of the processing
- ✓ A description of the categories of data subjects and of the categories of personal data
- ✓ The categories of recipients to whom the personal data have been or will be disclosed
- ✓ Where possible, the envisaged time limits for erasure of the different categories of data

10 SECURITY OF PERSONAL DATA

Record Personal data must be safeguarded from unauthorized or unlawful processing and access, accidental loss, destruction, or damage. This applies regardless of whether data is processed electronically or in paper form. Prior to the introduction of new methods of data processing, particularly new IT systems, technical and organizational measures to

protect personal data must be defined and implemented. These measures must be based on the state of the art, the risks of processing, and the need to protect the data (determined by the process for information classification).

11 DATA PROTECTION CONTROL

Compliance with this Data Protection Policy and the applicable data protection laws is checked regularly with audits and other controls. The results of the data protection controls must be reported to the Company's Board of Directors. On request, the results of data protection controls will be made available to the responsible data protection authority.

12 DATA PROTECTION INCIDENTS

12.1 NOTIFICATION OF SUPERVISOR

All employees must inform their supervisor immediately about cases of violations against this Data Protection Policy or other regulations on the protection of personal data (data protection incidents).

12.2 NOTIFICATION OF DATA PROTECTION SUPERVISORY AUTHORITY

In the case of a personal data breach, the Company must without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

The notification referred to in the preceding paragraph of this Article shall at least:

- ✓ Describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned
- ✓ Communicate the name and contact details of the contact point where more information can be obtained
- ✓ Describe the likely consequences of the personal data breach
- ✓ Describe the measures taken or proposed to be taken by the Company to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

The Company shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with the GDPR and other applicable data protection law.

12.3 COMMUNICATION OF PERSONAL DATA BREACH TO THE DATA SUBJECT

If the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the Company must communicate the personal data breach to the data subject without undue delay.

The communication to the data subject referred to, shall not be required if any of the following conditions are met:

- ✓ The Company has implemented appropriate technical and organizational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorized to access it, such as encryption
- ✓ The Company has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialize
- ✓ It would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner

13 RESPONSIBILITIES AND SANCTIONS

The executive bodies of the Company are responsible for data processing in their area of responsibility. Therefore, they are required to ensure that the legal requirements, and those contained in this Data Protection Policy, for data protection are met (e.g. national reporting duties). Management staff are responsible for ensuring that organizational, HR, and technical

measures are in place so that any data processing is carried out in accordance with this Data Protection Policy. Compliance with these requirements is the responsibility of the relevant employees.

Improper processing of personal data, or other violations of the data protection laws, can be criminally prosecuted in many countries and result in claims for compensation of damage.

14 REVISION HISTORY

Revision#	Date	Author(s)	Description
01	May 21, 2018	Katja Ekqvist	Initial availability

12 APPENDICES

None