PRIVACY POLICY of IRCBB

This Policy sets out our standards for the management and protection of Personal Data. They apply to our activities in any country for any activity that includes information about individuals we conduct in each of our affiliates and any domains (including any successor) including, but not limited to, research, production, business activities, corporate support, and data transfers necessary to carry out the above activities, including but not limited to:

Research and Production: initiation, management and funding of research studies / evaluation and involvement of researchers, members of the Science and Ethics Committee and partners to support research studies and development of our products / recruitment for research studies / evaluation of safety, efficiency and quality our growing and commercially available products / adherence to our commitment to the safety and quality of our products, including management and reporting adverse effects and complaints about product quality / submission of an application for authorization and registration of our products to the principles of health regulations / compliance with relevant legal, regulatory or ethical requirements.

Commercial activities: market evaluation of our products / advertising, marketing, sale, and delivery of our products / services / communication with our clients and other end users of our products / services / sponsorship and conduct of events / evaluation and encouragement of partners us to support our commercial activities / compliance with relevant legal, regulatory or ethical requirements.

Corporate support: Recruiting, recruiting, managing, developing, communicating with and compensating employees / providing benefits to employees and their protected family members / conducting employee performance appraisals and talents / providing education and other educational and development programs / conducting disciplinary procedures and employee complaint handling / management of ethics and privacy concerns and conduct of investigations / management and assurance our physical and virtual assets and infrastructure / procurement and payment for products and services / fulfilling our commitments on environment, health and safety and corporate responsibility / media communication / and compliance with relevant legal, regulatory or ethical requirements.

This Policy also applies to all individuals whose data we process, including but not limited to customers, prospective, current, and former employees and their dependents, members of the Ethics Committee, partners, investors and shareholders, government employees and other stakeholders. All Employees and Executives have significant privacy responsibilities that they must adhere to. We recognize that unintentional errors and misstatements in data protection can cause risks to the privacy of individuals and risks to IRCBB's reputation, processes, compliance, and finances. Every employee and other individuals processing data about IRCBB are responsible for understanding and observing their obligations under this Policy and the applicable laws.

Our Values and Standards on Privacy

We respect our values of privacy in everything we do and involve people, including how we apply privacy standards. The four privacy values include:

Respect. We recognize that privacy concerns are often related to the essential questions of who we are, how we see the world and how we define ourselves. So, we strive hard to respect the perspective and interests of individuals and societies and to be fair and transparent in how we use and share information about them.

Confidence. We know that trust is vital to our success, and so we are working hard to create and maintain customer, employee, patient, and other stakeholders' confidence in respecting and protecting information related to them.

Prevent damage. We understand that misuse of human-related information can create tangible and intangible harm to individuals, so we try to prevent physical, financial damage, damage to their reputation or other privacy-related harm.

Compliance. We have learned that laws and regulations are not always consistent with the rapid advances in technology, data flow and associated changes in risks and expectations of privacy. So, we strive hard to comply with the spirit and rules of privacy and data protection laws in a way that demonstrates consistency and operational proficiency for our business operations at a global level. We integrate our privacy standards into all activities, processes, technologies, and relationships with third parties using Personal Data. We design privacy controls on our processes and technologies that are consistent with our values and privacy standards and the applicable law. The 8 privacy principles outlined below summarize the privacy standards and the basic requirements for high-level processes, activities, and support technologies.

Privacy Policy Our Basic Commitments

1. Necessity – Before collecting, using, or distributing Personal Data, we define and record the specific, legitimate business purpose for which this is necessary. We define and record the time for which Personal Data is needed for these specified business purposes. We do not collect, use, or share more Personal Data than needed, or retain Personal Data in an identifiable form for longer than is necessary for these specified business purposes. Anonymize data when business requirements make it necessary for information about the activity or process to be withheld for a longer period. We ensure that these necessary requirements are embedded in any supportive technologies and that the third person supporting the activity or processing is informed.

2. Justice – We do not process Personal Data in ways that are unfair to the data subjects. We determine whether the proposed collection, use, or other form of processing of Personal Data constitutes a risk for actual or indefinite harm to individuals, in accordance with the Privacy Preventing Privacy Act. If the nature of the data, types of people or activity contain an inherent risk of actual or indefinite harm to individuals, we ensure that the risk of harm does not outweigh the relative benefits for these individuals or our mission to save and to improve human lives. Where risk is inversely related to benefits for individuals, we treat sensitive or personal data only with the explicit consent of individuals or as required or expressly permitted by existing laws. We record the risk analysis and design any required mechanisms to obtain and record evidence that demonstrates consensus on assistive technologies.

3. Transparency – We do not process Personal Data in ways or purposes that are not transparent. All persons whose Personal Data are processing with this Policy will be entitled to a copy of this Policy. We will make available copies of this Policy online at www.ircbb.com. The Data Protection Officer will provide digital and/or physical copies of this Policy upon request to the addresses listed below. When collecting Personal Data directly from individuals, we inform them through a clear, distinct, and easily accessible privacy notice or similar means before collecting information about (1) the corporate entity or entities responsible for processing, (2) the type of data to be collected, (3) the purposes for which it is to be used, (4) the person to whom it will share, including any claims that may be disclosed to personal data following legitimate requests from public authorities, (5) (6) how individuals can ask questions, express concern or exercise their rights regarding the data, and (7) the electronic link of this Policy wherever possible and appropriate. When collecting Personal Data from other sources and not necessarily management, prior to obtaining the data, we verify in writing that the data provider has informed individuals about the ways and purposes with which the IRCBB intends to use the information. If the written verification cannot be obtained from the provider, we only use anonymous data, or before we use Personal Data, we inform individuals affected by a privacy notice or similar means of (1) the corporate entity or entities responsible for processing, (2) the type of data to be collected, (3) the purposes for which it will be used, (4) with whom to share, including any claims to be revealed. (5) how long they will be withheld, (6) how individuals can ask questions, express concern, or exercise their rights with respect to the data, and (7) the electronic link to this Policy wherever possible and appropriate. We ensure that the necessary transparency mechanisms, including where possible mechanisms supporting individual rights requests, are introduced into assistive technologies, and that third parties

supporting the activity or processing do not process individual data in ways that are inconsistent with what has been tell people, through privacy notice or other verifiable means, how we and others who work for us will use the data.

4. Purpose Restriction – We use Personal Data only in accordance with the principles of Necessity and Transparency. If new legitimate corporate purposes are already identified for Personal Data already collected, we ensure that either the new business purpose (including a substantially similar purpose) is compatible with the purpose as described in the privacy notice or other transparency mechanism previously provided to the individual, either we obtain the consent of the individual for the new use of his or her Personal Data. We do not apply the above principle to anonymous data, or where we use Personal Data solely for the purpose of historical and scientific research, and (1) an Ethics Review Committee or other competent auditor has determined that the risk of such use for privacy or other rights of individuals is acceptable and (2) there is respect for existing legislation. We ensure that purpose limitation constraints are embedded in assistive technologies, including any reporting and downstream data sharing capabilities.

5. Quality of Data – We keep Personal Data accurate, complete, and unaltered as delivered to us by the same customer/business.

6. Security – Incorporate safety valves to protect your Personal Data and Sensitive Data from loss, misuse, and unauthorized access, disclosure, or destruction. We have implemented an analytical information security program and we apply security controls based on the sensitivity of the information and the size of the risk of the activity, considering the best practices of modern technology and the cost of implementation. Our operational safety policies include, but are not limited to, business continuity and disaster recovery standards, identity and access management, information classification, information security incident management, network access control, physical security, and risk management.

7. Data Transfer – We are responsible for preserving the privacy of Personal Data when it is transferred from or to other agencies or state borders. (1) We only transfer Personal Data or permit processing by third parties if the following conditions are met, and we are responsible for ensuring that third parties we partner meet these requirements: If the third person's role is to process Personal Data for or on behalf of IRCBB before the third person receives the Personal Data, we: (1) complete the privacy review to evaluate the privacy practices and risks associated with these third parties, (2) we obtain warranties by contract from these third parties that we will process Personal Data in accordance with IRCBB's instructions and in accordance with this Policy, including, without limitations of the 8 Privacy Principles and other standards set forth in this Policy and existing legislation, and will promptly notify IRCBB of any Privacy Event, including any inability to comply with the standards set forth in this Policy and the existing law, or Security Event, and will work together to timely remedy any documented incident and address the individual rights as defined in Section 2 below, and that will allow IRCBB to review and supervise their practices during processing to comply with these requirements. Additionally, if the third person processes Personal Data originating from a country or territory with legislation restricting the transfer of Personal Data, we will ensure that the transfer to the third party meets the conditions for cross-border transportation described below in Section 2. Where a from our affiliates only acts on behalf of another subsidiary of IRCBB for the processing of Personal Data, and where required by the Law, these subsidiaries of the IRCBB we will perform an internal data processing in accordance with Principle 8 of this Policy. If the third person's role is to provide Personal Data to IRCBB, before we obtain the Personal Data from the third party, we ensure that the Transparency Requirements are met for the collection of Personal Data from other sources and not specifically under the supervision of IRCBB, and we obtain warranties by third party contract that it does not violate any Law or the rights of any third party with the provision of Personal Data to IRCBB. If the third party's role is to obtain from IRCBB data for processing that is not specifically under IRCBB's control, before we deliver the data to the third party, we ensure that the data is anonymized and we obtain written guarantees from the third party person that he will use the data only for the operational purposes specified in the agreement and in accordance with existing legislation and that he will not attempt to reverse the anonymity process. (2) We transfer Personal Data cross-

border from or on behalf of IRCBB in accordance with this Policy. We will apply this Policy to transfers of Personal Data from any other country or territory with legislation restricting the transfer of Personal Data.

8. Legally Permissible – We process Personal Data only if it complies with the requirements of applicable law. While the other 7 privacy principles and the terms of the Rights of Rights described below are intended to ensure that the most privacy and data protection laws applicable to our industry worldwide are met, countries need to meet additional conditions, including but not limited to: Where necessary, we will obtain specific forms of consent to process specific Personal Data, including, but not limited to, approval of processing by labor councils or other trade unions. Where necessary, we will process the processing of Personal Data with the applicable privacy or data protection regulator. Where necessary, we will further limit the data retention periods for the Personal Data. Where appropriate, we will enter into agreements that include special contract clauses, including agreements for cross-border data transfers to third parties. Where necessary, we will disclose personal data following legitimate requests from the public authorities, including the satisfaction of requests related to national security or security authorities. In the event of a conflict between this Policy and existing legislation, the standard that provides more protection to individuals will prevail. We will address promptly requests for individual rights to access, correct, modify, or delete any Personal Data or objection to the processing of Personal Data. Access, Correction and Deletion – Individuals have the right to access Personal Data about them, and to correct, modify or delete any Personal Data that is inaccurate, incomplete, or obsolete. We will approve all individuals requests for access, correction, and deletion of Personal Data. If an application for access, correction or deletion is defined by existing Legislation that provides greater protection for individuals, we will ensure that the additional conditions are met under Legislation. Choice – In accordance with privacy principles for "Respect" and "Trust", we approve individual requests for objection to the processing of Personal Data, including, but not limited to, the option not to participate in programs or activities that individuals have previously agreed to participate in the processing of Personal Data about them for direct marketing purposes for communication that targets them and which is based on Personal Data, and for any evaluation or decision making information about them, which has the potential to influence them significantly, through the use of algorithms or automation. Except and where prohibited by law, we may deny the choice where a particular application may hamper the ability of the IRCBB to: (1) comply with the law or a moral obligation, including the case that we are obliged to disclose personal data in response (2) investigate, defend or seek legal claims, and (3) conclude contracts, deal with relationships, or (3) perform other permitted business activities in accordance with the principles of Transparency and purpose limitation and introduced the basis of those data associated with them. Within fifteen working days of any decision to refuse a request for selection in accordance with this Policy, we will record and communicate the decision to the applicant. We will respond in a timely manner, and we will scale all questions related to privacy, complaints, concerns and any Privacy Event or Security Event. Any person whose Personal Data we process within the scope of this Policy may ask questions, complain, or express concerns to IRCBB at any time, including the request to provide a list of all our affiliates subject to this Policy. We expect that our employees and other individuals working on behalf of IRCBB will provide early notice if they have reason to believe that an applicable law may prevent them from complying with this Policy. Any question, complaint, or concern from an Individual or any notice from an employee or other person working on behalf of IRCBB should be addressed to the Data Protection Officer: by email: info@ircbb.com responsible: Prof. Kappos LD. Employees and contractors are required to inform their Data Protection Officer in time for any questions, complaints, or concerns about privacy practices. The Data Protection Officer will review and investigate or work with the Legal Service to investigate all inquiries, complaints, or concerns related to IRCBB's privacy practices, whether taken directly by our employees or other individuals or third parties, including, but not limited to, regulatory agencies, liability officers or other government authorities. We will respond to the person or entity who raised the question, complaint, or concern in IRCBB within thirty (30) or within a maximum of sixty (60) calendar days, except that a law or applicant / third party requires a response within a shorter period; unless conditions, such as a parallel state survey, require a longer period. In this case, the person or applicant / third party will be notified in writing as soon as possible of the general nature of the circumstances contributing to the delay. The Data Protection Officer, in cooperation with the Law Office and the Compliance Office, will work with the privacy regulator in response to any investigation, inspection or investigation.

Terms that you need to know

Anonymous. Changing, cutting, eliminating, or otherwise restricting or transforming Personal Data to make it impossible for them to be used to identify, locate, or communicate with the individual. Legislation. All laws, rules, regulations, and mandates of law enforcement in any country that IRCBB operates or in which Personal Data is processed by or on behalf of IRCBB. IRCBB, its subsidiaries, apart from the joint ventures in which IRCBB participates.

Privacy. All data for a recognized or unidentified individual, including data that the person identifies or could be used to identify, identify, track, or communicate with him. Personal Data also includes instant identification information such as name, identification number or unique job title, and indirect identification information such as birthdate, unique mobile or portable identification number, telephone number and encoded data.

Privacy Event. Violation or violation of this Privacy Policy or privacy or data protection law and includes a Security Event. Determining whether a privacy event has taken place and whether it has a physical occurrence will be done by the Data Protection Officer and the Legal Department/Compliance Department. Processing. Performing any process or series of processes in human data, with or without automated means, including, but not limited to, collection, recording, organization, storage, access, adaptation, conversion, retrieval, counseling, use, evaluation, analysis, reference, distribution, disclosure, and dispersion, transmission, mood, alignment, combination, inhibition, deletion, erasure, or destruction.

Security Incident. Access by an unauthorized person to Personal Data or disclosure to an unauthorized person or the reasonable suspicion of that this has happened. Access to Personal Data by or on behalf of IRCBB. By without the intention of violating this Policy is not a Security Event, provided that such Personal Data was then used and disclosed only as permitted by this Policy.

Sensitive data. Any type of data relating to people with intrinsic risk of potential harm to individuals, including data that is legally defined as sensitive, including, but not limited to, health, inheritance, race, ethnic origin, religion, policies or philosophical beliefs or beliefs, criminal records, precise geographic location information, bank or other financial account numbers, state registration numbers, minor sex, sex with the trade unions, security, social security and other employer or state benefits.

Third person. Any legal entity, organization or person not belonging to IRCBB. By, or for which IRCBB has no controlling interest or does not work for IRCBB. Unless expressly determined by this Policy, no subsidiary or business of IRCBB is required to meet the requirements of a third party under this Policy as all affiliates and domains are required to process human data in accordance with this Policy, including cases where one of our subsidiaries supports one or more of our affiliates while processing.

Changes to this Policy. This Policy may be reviewed occasionally in accordance with the requirements of existing legislation. Whenever this Policy changes physically, a notice will be posted on IRCBB's website (www.ircbb.com) for 60 days. Date of effect 20 May 2018 (u/d 2023).