Data Protection Policy

Policy Number:		
Version Number: 1	Issue Date: 22 July 2020	Effective Date: 1 August 2020
Authorized by:	Name: Title:	
Policy Owner : Ioannis Giannakakis	The Policy Owner is responsible for periodically reviewing and updating this Policy so as to reflect regulatory, best practice, and business developments.	

ANDROMEDA SEAFOOD DATA PRIVACY POLICY

Our Group strives to conduct its business in accordance with our privacy values because we believe they demonstrate our unwavering commitment to ethical and responsible practices. We recognize that innovation and new technology drive continual change in risks, expectations and laws, so we follow privacy accountability standards and aim to promptly adapt how we apply them in response to those changes.

This Policy defines our standards for management and protection of Personal Information by or on behalf of our company that directly or indirectly originates from any country in the European Economic Area ("EEA"), and globally and is transferred to any other country, including transfers between the EEA.

It applies to our operations in every country, to every activity involving information about people that we conduct in every subsidiary and every division (including by any successors to our business), including, but not limited to aquaculture.

This Policy also applies to all people about whom we process information, including, but not limited to, customers; prospective, current and former employees and their dependents, ethics committee members, business partners, investors and shareholders, government officials, and other stakeholders.

Definitions

Throughout this Policy, defined terms are capitalized and have the following meanings:

- **Anonymized.** The alteration, truncation, obliteration or other redaction or modification of Personal Information so as to render it incapable of being used to identify, locate or contact an individual.
- **Law.** All applicable laws, rules, regulations, and orders of opinions having the force of law in any country in which our company operates or in which Personal Information is processed by or on behalf of our company
- **Our Group of Companies . Andromeda Seafood Group** and its successors, subsidiaries and divisions, excluding joint ventures to which our company is a party.
- **Personal information.** Any data about an identified or identifiable individual, including data that identifies an individual or that could be used to identify, locate, track, or contact an individual. Personal information includes both directly identifiable information such as a name, identification number or unique job title, and indirectly identifiable information such as date of birth, unique mobile or wearable device identifier, telephone number as well as key-coded data.
- **Privacy incident.** A violation or breach of this Policy or a privacy or data protection law, and includes a Security Incident. Determinations of whether a privacy incident has occurred and whether it is material shall be made by the local Data Protection Officer and the Group/Regional Legal.
- **Processing.** Performing any operation or set of operations on information about people, whether or not by automatic means, including, but not limited to, collecting, recording, organization, storage, access, adaptation, alteration, retrieval, consultation, use, evaluation, analysis, reporting, sharing, disclosure, and dissemination, transmission, making available, alignment, combination, blocking, deleting, erasure or destruction.
- **Security incident.** Access by or our company's reasonable belief of any access or use by, or any disclosure by or to, an unauthorized person to Personal Information. Access to Personal Information by or on behalf of our company without the intent to violate this Policy does not constitute a Security Incident, provide that the Personal Information accessed is further used and disclosed solely as permitted by this Policy.
- **Sensitive information.** Any type of information about people that carries an inherent risk of potential harm to individuals, including information defined by law as sensitive, including, but not limited to information related to health, genetics, race, ethnic origin, religion, political or philosophical opinions or beliefs, criminal history, precise geo-location information, bank or other financial account numbers ,Government-issued identification numbers, children who are minors, sex life, trade union affiliation, insurance, social security and other employer or government-issued benefits.
- **Third party.** Any legal entity, association or person that is not owned by our company, or in which our company does not have a controlling interest, or who is not employed by our company. Except as expressly set forth in this Policy, no subsidiary or division of our company shall be required to meet the requirements of a third party under this policy as all subsidiaries or divisions are required to process information about people in accordance with this Policy, including in circumstances where one of our company subsidiaries supports one or more other subsidiaries of our company in the processing.

All Company Employees and Senior Leaders have core privacy responsibilities they must uphold.

We recognize that inadvertent errors and misjudgments related to protection of information about people can create privacy risks for individuals and reputational, operational, financial and compliance risks for our Group . Every employee of our company, and others who process information about people for our company, is accountable for understanding and upholding their obligations under this Policy and applicable Laws.

Our Privacy Values and Standards

We uphold our privacy values in everything we do involving people including how we apply our privacy standards. Our four privacy values include:

- **Respect**

We recognize that privacy concerns often relate to the essence of who we are, how we view the world and how we define ourselves, so we strive to respect the perspectives and interests of individuals and communities and to be fair and transparent in how we use and share information about them.

- **Trust**

We know that trust is vital to our success, so we strive to build and preserve the trust of our customers, employees, patients and other stakeholders in how we respect privacy and protect information about people.

- **Prevent Harm**

We understand that misuse of information about people can create both tangible and intangible harms for individuals, so we seek to prevent physical, financial, reputational and other types of privacy harms to individuals.

- **Comply**

We have learned that laws and regulations cannot always keep pace with the rapid change in technologies, data flows, and associated shifts in privacy risks and expectations, so we strive to comply with both the spirit and letter of privacy and data protection laws and regulations in a manner that drives consistency and operating efficiency for our global business operations

1. We embed our privacy standards into all activities, processes, technologies and relationships with third parties that use Personal Information. We design privacy controls into our processes and technologies that are consistent with our privacy values and standards and applicable law. **Our 8 privacy principles** set forth below summarize our privacy standards and core requirements for processes, activities and their supporting technologies at a high level.

Privacy Principle	Our Core Commitments
1. **Necessity** – Prior to collecting, using, or sharing Personal Information, we define and document the specific, legitimate business purposes for which it is needed.	• We determine and document how long Personal Information is needed for those defined business purposes. • We do not collect, use or share more Personal Information than is needed or retain it in identifiable form for longer than is needed for those defined business purposes. • We anonymize the data when business requirements necessitate that information about the activity or process is retained for a longer period of time. • We ensure that these necessity requirements are designed into any supporting technology and that they are communicated to third parties supporting the activity or process.
2. **Fairness**–We don't process Personal Information in ways that are unfair to the people to whom those data relate.	• We determine whether the proposed collection, use or other processing of Personal Information presents a risk of tangible or intangible harm to individuals in accordance with our privacy value to *Prevent Harm*. • If the nature of the data, types of people, or the activity presents an inherent risk of tangible or intangible harm to individuals, we ensure that the risk of harm is outweighed by a corresponding benefit to those individuals or to our mission of saving and improving lives. • Where the risk is disproportionate to the benefits to individuals, we only process the Sensitive Information or Personal Information with the explicit consent of the individuals or as expressly required or expressly permitted by applicable law. • We document the risk analysis and design any required mechanisms to obtain and document evidence of consent into supporting technologies.
3. **Transparency** – We don't process Personal Information in ways or for purposes that are not transparent.	• All individuals about whom Personal Information is Processed under this Policy shall have a right to a copy of this Policy. We will make copies of this Policy available online https://www.andromedagroup.eu The Data Protection Officer will provide electronic and/or paper copies of this Policy upon request to the addresses listed below in Section (3) of this Policy . • ***When Personal Information is collected directly from individuals***, we inform them through a clear, conspicuous, and easily accessible privacy notice or similar means prior to collecting the information of (1) the company entity or entities responsible for the processing, (2) what information will be collected, (3) the purposes for which it will be used, (4) with whom it will be shared , including any requirements to disclose Personal Information in response to lawful requests by

	government authorities, (5) how long it will be retained, (6) how they can ask a question, raise a concern or exercise their rights related to the information, and (7) a link to this Policy, where possible and appropriate. • ***When Personal Information is obtained through observation, sensors, or other indirect means***, it may not be possible to provide a privacy notice directly to the individual at the time the information are collected. In such cases, we assure transparency to the individual through other means, such as posted or printed on the device or materials associated with the device that will obtain the information. • ***When Personal Information is collected from other sources and not specifically at the direction of our company***, prior to obtaining the information, we verify in writing that the provider of the information has informed individuals of the ways and purposes for which our company intends to use the information. If written verification cannot be obtained from the provider of the information, we use only anonymized information, or prior to using Personal Information, we inform the affected individuals through a privacy notice or similar means of (1) the entity or entities of our company responsible for processing the information, (2) what information our company plans to use, (3) the purposes for which our company plans to use it, (4) with whom our company plans to share it, (5) how long plans to retain it, (6) how they can ask a question, raise a concern or exercise their rights, and (7) a link to this Policy, where possible and appropriate. • We ensure that the necessary transparency mechanisms, including, where possible, mechanisms that support individual rights requests, are designed into supporting technologies, and that third parties supporting the activity or process do not process information about people in ways that are inconsistent with what individuals have been told through a privacy notice or other verifiable means that we and others working for us will do with the information.
4. **Purpose Limitation** –We only use Personal Information in accordance with the Necessity and Transparency principles.	• If new legitimate business purposes are identified for Personal Information that previously was collected, we either ensure that the new business purpose is compatible with, including materially similar to a purpose described in a privacy notice or other transparency mechanism that previously was provided to the individual, or we obtain the individual's consent for the new use of Personal Information. • We do not apply this principle to anonymized information or

	Where we use Personal Information solely for historical and scientific research purposes • We ensure that purpose limitation restrictions are designed into any supporting technology, including any reporting capabilities and downstream data sharing.
5. **Data Quality** – We keep Personal Information accurate, complete and current consistent with its intended use.	• We ensure that periodic data review mechanisms are designed into supporting technologies to validate the data accuracy against source and downstream systems. • We ensure that Sensitive Information is validated as accurate and current prior to its use, evaluation, analysis, reporting or other processing that presents a risk of unfairness to people if inaccurate or outdated data are used. • Where changes are made to Personal Information by our company or third parties working for our company, we ensure that those changes are timely communicated where reasonably possible.
6. **Security** – We implement safeguards to protect Personal Information and Sensitive Information from loss, misuse, and unauthorized access, disclosure, alteration or destruction.	• We have implemented a comprehensive information security program and we apply security controls that are based on the sensitivity of the information and the risk level of the activity, taking into account current technology best practices and the cost of implementation. Our functional security policies include, but are not limited to, standards on business continuity and disaster recovery, encryption, 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 and we preserve the privacy protections for Personal Information when it is transferred to or from other organizations or across country borders.	(1) We only transfer Personal Information to or allow it to be processed by third parties if the following requirements are met and we are liable for ensuring that the third parties we engage meet these requirements: • ***If the role of the third party is to process Personal Information for or on behalf of our company***, before providing Personal Information to the third party or engaging the third party, we: (1) complete privacy due diligence to evaluate the privacy practices and risks associated with those third parties, (2) obtain contractual assurances from those third

parties that they will process Personal Information pursuant to our company's instructions, and in accordance with this Policy, including without limitation all 8 Privacy Principles and the other standards set forth in this Policy, and applicable Laws, that they will notify our company promptly of any Privacy Incident, including any inability to comply with standards set forth in this Policy and applicable Laws, or Security Incident, and cooperate to promptly remediate any substantiated Incident and to address the individual rights set forth in Section 2 below, and that they will permit our company to audit and monitor their practices for the duration of the processing for compliance with these requirements. Additionally, if the third party processes Personal Information that originates in a country or territory with a law that restricts the transfer of Personal Information, we will ensure that the transfer to the third party meets the requirements for cross- border data transfer described in (2) below. Where one of our company subsidiaries acts solely on behalf of another of our company subsidiaries in processing Personal Information, where required by Law, those subsidiaries of our company will execute an internal data processing agreement in accordance with Principle 8 of this Policy.

- ***If the role of the third party is to supply Personal Information to our Group***, before obtaining Personal Information from the third party, we ensure that the Transparency requirements for collecting Personal Information from other sources and not specifically at the direction of our company are met, and we obtain contractual representations from the third party that it is not violating any Law or the rights of any third party by providing Personal Information to our company.
- ***If the role of the third party is to receive information from our Group for processing that is not specifically at the direction of our company***, before providing information to the third party, we ensure that the information has been anonymized, and we obtain written assurances from the third party that they will use it only for business purposes defined in the agreement and in accordance with applicable laws, and that they will not attempt to re-identify the information.

(2) We transfer Personal Information across country borders by or on behalf of our company in accordance with this Policy. We will apply this Policy to transfers of Personal Information from any other country or territory with a law that restricts the transfer of Personal Information.

8. **Legally Permissible** – We only process Personal Information if the requirements of applicable laws have been met.	• While the other 7 privacy principles, as well as the Individual Rights requirements described below, are intended to ensure that the requirements of most privacy and data protection laws that apply to our business around the world have been met, in some countries, we need to meet additional requirements, including but not limited to the following: 1. Where required, we will obtain specific forms of consent for certain processing of Personal Information, including but not limited to, approval of the processing by works councils and other labor unions; 2. Where required, we will register processing of Personal Information with the applicable privacy or data protection regulatory authority; 3. Where required, we will further limit data retention periods for Personal Information; 4. Where required, we will enter into agreements containing specific contractual clauses, including agreements for cross - border data transfer to third parties; and 5. Where required we will disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements. • In the event of a conflict between this Policy and an applicable law, the standard that provides more protection to individuals will prevail.

2. We will promptly address individual rights requests to access, amend, correct or delete Personal Information or to object to the processing of Personal Information about them.
    - **Access, Correction and Deletion** – Under the European Data Protection laws and the General Data Protection Regulation ("GDPR") in the European Union, individuals have a right to access Personal Information about themselves, and to amend, correct or delete Personal Information that is inaccurate, incomplete or outdated. We will honor all requests to access, correct and delete Personal Information from all individuals. If a request for access, correction or deletion is governed by an applicable Law that provides greater protection to individuals, we will ensure that the additional requirements of that Law are met.
    - **Choice**–Consistent with our privacy values of "Respect" and " Trust," we honor individual requests to object to Personal Information processing, including, but not limited to opting out of programs or activities in which they previously agreed to participate, processing of Personal Information about them for direct marketing communications, communications targeted to them based on Personal Information about them, and any evaluation of or decisions about them, which has the potential to significantly affect them, made by use of automation or algorithms.
    - Except where prohibited by Law, we may deny the choice where a particular choice request would impede our company in its ability to: (1) comply with a Law or an ethical obligation including where we are required to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements, (2) investigate, make or defend legal claims, and (3) perform contracts, administer relationships, or engage in other permitted business activities that are consistent with the Transparency and Purpose Limitation principles and were entered into in reliance on the information about people in question. Within fifteen business days of any decision to deny a choice request in accordance with this Policy, we will document and communicate the decision to the requestor.
3. We will promptly respond to and escalate all privacy-related questions, complaints, concerns and any potential Privacy Incident or Security Incident.
    - Any individual about whom we process Personal Information within the scope of this Policy can raise a question, complaint or concern to our company at any time, including a request for a list of all subsidiaries of our company that are subject to this Policy. We expect that our employees, and others who work on behalf of our company, provide prompt notice if they have a reason to believe that an applicable Law may prevent them from complying with this Policy. Any question, complaint or concern raised by an Individual, or any notice provided by an employee or any other person who works on behalf of our company, should be directed to the Data Protection Officer:
    -
        - By mail to : ethics@andromedagroup.eu
        - By fax to: +34 964 586 321
        - By postal mail To Andromeda Seafood S.L C/Manuel Sanchis Guarner 3, Vall D´Uixo, Castellón, (España)

- Employees and contractors are required to promptly inform the local Data Protection Officer for their business area, of any questions, complaints or concerns related to our company's privacy practices.
- The Data Protection Officer will review and investigate, or will work with, Legal to investigate, all questions, complaints or concerns related to our company's privacy practices, whether received directly from employees or other individuals or through third parties, including, but not limited to regulatory agencies, accountability agents and other government authorities. We will respond to the individual or entity that raised the question, complaint or concern to our company within thirty (30) calendar days unless a Law or the third party requestor requires a response in a shorter period of time or unless circumstances, such as a concurrent government investigation, require a longer time period, in which case the individual or third party requestor will be notified in writing as soon as practicable of the general nature of the circumstances contributing to the delay.
- The Data Protection Officer, in coordination with Legal, will cooperate in response to any inquiry, inspection or investigation of a privacy regulatory authority.
- For complaints that cannot be resolved between our company and the individual who raised the complaint, our company has agreed to participate in the following dispute resolution procedures in the investigation and resolution of complaints to resolve disputes pursuant to this Policy, however, at any time, individuals resident in the EEA or individuals about whom Personal Information is subject to the data protection Law of the EEA and transferred outside of the EEA,
- All individuals residing in the EEA, or individuals about whom Personal Information is subject to the data protection Law of the EEA and transferred outside of the EEA, about whom information is processed pursuant to this Policy have the right under this Policy, at any time, to enforce the requirements of this Policy as third party beneficiaries, including the right to bring a Judicial action to seek remedies for breach of his or her rights under this Policy and the right to receive an award for damages resulting from such breach.
    - In the courts or with the data protection authority in the EEA country from which Personal Information about them was transferred, or
    - In the courts of Spain or in local Data Protection Authority (DPA)

- Our company will respond to the individual or entity that raised the question, complaint or concern to our company not later than **thirty(30) calendar days** unless a Law or the third party requestor requires a response in a shorter period of time or unless circumstances require a longer time period, in which case the individual or third party requestor will be notified in writing.