Data Protection Policy

WW Legal Dept.

Rev. Doc.: v.2
Date: February 16, 2018
Dept.: WW Legal
Contact: Aaron Mendelsohn
Pages: 1 of 5

Ingram Micro, its subsidiaries and affiliated companies ("**Ingram Micro**") respects employee, customer, supplier, reseller, and other third party (collectively, a "**Data Subject**") Personal Data, and strives to collect, use and disclose personal information in a manner consistent with the laws of the countries in which it does business.

INTRODUCTION

Ingram Micro is committed to protecting the Personal Data that it gathers concerning its prospective, current and former employees for management, human resources, and payroll purposes, and customers, suppliers, resellers, and other third parties in the course of Ingram Micro's business.

This global Data Protection Policy ("**Policy**") is designed to establish a clear and comprehensive corporate policy for handling Personal Data. Each Ingram Micro entity is considered a "controller" under data protection laws for the Personal Data it directly collects from Data Subjects. As a controller, each Ingram Micro entity collects and processes Personal Data for which it establishes a legitimate business purpose and has implemented adequate security measures. Ingram Micro entities may also process data as "processor", assigned by another "controller" – for example a customer. In that respect Ingram Micro may have both contractual and regulatory requirements with regard to the collection and processing of Personal Data.

This Policy includes a list and the description of the processing and the security measures for protecting Personal Data.

For questions and examples regarding this Policy please see the Frequently Asked Questions (FAQ) available here.

SCOPE

Ingram Micro strives to collect, use and process Personal Data in a manner consistent with the privacy and personal data protection laws of the countries in which it does business. Because of the differences among these jurisdictions, Ingram Micro has adopted this Policy and a data protection program that creates a common core of values, policies and procedures intended to achieve compliance, supplemented with alternative or additional policies or implementation procedures applicable in those jurisdictions with unique requirements.

This Policy establishes a worldwide standard within Ingram Micro for collecting, using and protecting Personal Data in any form – whether oral, electronic or written.

This Policy must be implemented and followed in all Ingram Micro businesses, functions, regions, and subsidiary companies, including those located in jurisdictions in which the privacy protections provided by this Policy are not legally required. Since Ingram Micro business entities must always comply with relevant local laws and regulations, such laws and regulations are to be followed even if they conflict with certain aspects of this Policy and related standards.

This Policy applies globally to all Ingram Micro operating companies. Based on applicable regulations or local risks, Ingram Micro entities may have more detailed and specific policies on a country or regional level as approved by the Global Chief Data Privacy Officer, Regional Compliance Officer, and the General Counsel responsible for the particular country operation.

This Policy is to be followed not only internally, but also by all Processors, agents, temporary staff, contractors, service providers and consultants in their handling and processing of Personal Data on behalf of Ingram Micro, subject to the terms of appropriate processing agreements. Violation of this Policy may lead to disciplinary measures or contractual actions, up to and including termination.

DEFINITIONS

"**Processor**" means any Employee and third party that processes, collects or uses Personal Data under the instructions of, and solely for, Ingram Micro or to which Ingram Micro discloses Personal Data for use on Ingram Micro's behalf.

"**Ingram Micro,**" means Ingram Micro, its successors, affiliates and subsidiaries.

"Employee" means any prospective or current employee and any individual with a current or former employment contract with Ingram Micro.

"**Personal Data**" means any information or set of information that identifies or could identify any individual. Personal Data does not include information that has been made anonymous or aggregated information. Personal Data includes, but it is not limited to, Sensitive Personal Data (as defined below). Please see the FAQ for examples of Personal Data.

"Sensitive Personal Data" means certain sensitive categories of Personal Data, as defined by applicable laws. Definitions of sensitive information vary from country to country. European data protection laws treat certain categories of information as especially sensitive: information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life. Other categories of Personal Data are subject to additional protections under national law in some European countries: information about criminal history, civil judgments, administrative sanctions, government security measures, government-issued ID numbers, biometric data, genetic data, geo-location data, and personality profiling. Personal Data subject to legal and regulatory protection in the U.S. include information about age, gender, ethnicity, health, disability, sexual orientation, children under 13, credit history, bankruptcy, garnishments, genetics, Social Security Numbers, driver's license numbers, financial account and payment card details (in combination with PINs or other access codes), and other non-public financial and medical data. Ingram Micro only collects certain Sensitive Personal Data for the purpose of the performance of the employment agreement and/or in application of local law.

DATA PROTECTION PRINCIPLES

This Policy is built not just on individual country data protection laws but also on the internationally accepted data protection principles, or fair information practices, (collectively, the "**Principles**") established, among others, by the Organization for Economic Co-operation and Development (OECD), and global data protection and privacy laws, including, but not limited to the European Union's General Data Protection Regulation ("**GDPR**"), the United States' Health Insurance Portability and Accountability Act ("**HIPAA**"), and Canada's Personal Information Protection and Electronic Documents Act ("**PIPEDA**").

These Principles, and how Ingram Micro works to apply them, include the following:

COLLECTION:

Ingram Micro shall collect or obtain Personal Data only in a fair, non-deceptive and lawful manner and as needed for the purposes about which the Data Subject has been informed. Personal Data collection shall be consistent with local country and jurisdictional laws.

NOTICE:

When required by law and where Ingram Micro collects Personal Data directly or indirectly from a Data Subject, it will notify them at the time of data collection about: the type of information collected; purposes for which it collects and processes Personal Data about them as well as the legal basis for the collection; the types of third parties to which Ingram Micro communicates that Personal Data; the choices and means, if any, Ingram Micro offers a Data Subject

for limiting the use and disclosure of their Personal Data; who to contact at Ingram Micro about its practices concerning Personal Data; and any other circumstances required by local laws

CHOICE AND CONSENT:

When consent is required by law, Ingram Micro shall:

- Request the consent of the Data Subject in a clearly distinguishable manner, using an easily accessible form and clear and plain language;
- Inform the Data Subject of the consequences of their refusal to consent;
- Inform the Data Subject on how they can change their consent decisions;
- Obtain new consent if Personal Data will be used for a purpose other than originally disclosed to the Data Subject.

Ingram Micro will observe special regulations for consent by particular individuals, where required by local laws. For example, in various jurisdictions special requirements apply to the processing of Personal Data of children.

PROCESSING AND RETENTION:

Ingram Micro must collect, use, process, store, and/or retain Personal Data only for legitimate and lawful business purposes, which are in line with applicable regulatory requirements.

Personal Data must be retained and destroyed according to applicable laws.

DISCLOSURE AND TRANSFER:

Ingram Micro may share Personal Data with Processors for legitimate business purposes or for the purposes for which Personal Data was collected and will obtain assurances from Processors that they will safeguard Personal Data in a manner consistent with this Policy and the applicable laws and regulations. When sharing or transferring Personal Data outside of the European Economic Area, Ingram Micro shall apply the standard data protection clauses adopted by the European Commission to require Processors and sub-processors to adhere and abide to adequate data protection and information security standards.

SECURITY:

Ingram Micro will take reasonable precautions, including technical, administrative and physical measures to protect Personal Data from loss, misuse and unauthorized access, disclosure, alteration or destruction. As necessary, Ingram Micro will take additional precautions regarding the security of Sensitive Personal Data. Records containing Personal Data are considered Ingram Micro property and should be afforded confidential treatment at all times, regardless of whether these records are in electronic or paper form.

DATA INTEGRITY:

Ingram Micro will employ reasonable processes designed to keep Personal Data relevant to its intended use, accurate, complete and current. Ingram Micro will only use Personal Data in ways that are compatible with the purposes for which it was collected or subsequently authorized by the individual or by applicable legislative provisions.

ACCESS:

Data Subjects will have reasonable access to their Personal Data processed by Ingram Micro in order to correct, amend or delete Personal Data that is demonstrated to be inaccurate or incomplete, and as required by applicable laws and regulations. These requests may be made by contacting the local human resource manager, Global Chief Data Privacy Officer, Regional Compliance Officer, or local legal counsel.

Ingram Micro may limit or deny access to Personal Data as permitted by local laws or regulations or where the request is unreasonable. For example, Ingram Micro may limit an Employee access to Personal Data where the burden or expense of providing access would be disproportionate to the risks to the employee Personal Data or where the legitimate rights of persons other than the Employee would be violated.

ENFORCEMENT:

Ingram Micro is committed to enforcing ongoing compliance with this Policy and with applicable data protection laws, regulations and obligations.

Any questions or concerns regarding the use or disclosure of Personal Data should be directed to the local legal counsel, Regional Compliance Officer, or alternatively Global Chief Data Privacy Officer at the address listed in Section 03 below.

CROSS-BORDER TRANSFERS:

Like most international businesses, Ingram Micro has centralized certain aspects of its data processing and information systems in order to allow Ingram Micro to better manage its business. That centralization may result in the transfer of Personal Data from one country to another within the limits and subject to the requirements of the applicable laws. The countries where the information will be transferred may or may not have laws that seek to preserve the privacy of Personal Data. However, whenever Personal Data is transferred within Ingram Micro, Personal Data will be processed in accordance with the principles of this Policy and applicable laws, and Ingram Micro will ensure an adequate level of data protection according to the applicable laws of the country from which the data originates.

INCIDENT RESPONSE

Ingram Micro maintains an Incident Response Policy that defines the processes and procedures to detect, define and report a known or suspected security incident that impacts Personal Data. Where required by law Ingram Micro will notify Data Subjects of instances of unauthorized access, loss, or misuse of Personal Data.

DATA PROTECTION OFFICER

Where required by applicable law, Ingram Micro shall appoint a Data Protection Officer, or a similar function, that shall be responsible for enforcing this Policy, and addressing inquiries by Data Subjects and regulators.

CONTACT INFORMATION

Please submit questions or comments regarding this Policy or Ingram Micro's practices concerning Personal Data to:

Director, Global Chief Data Privacy Officer
Ingram Micro, Inc.
3351 Michelson Dr #100
Irvine, CA 92612
privacy@ingrammmicro.com

LIMITATIONS

While this Policy is intended to describe the broadest range of information processing activities globally, those processing activities may be more limited in some jurisdictions based on the restrictions of their laws. For example, the laws of a particular country may limit the types of Personal Data that Ingram Micro can collect or the manner in which Ingram Micro processes that information. In those instances, Ingram Micro adjusts its internal policies and practices to reflect the requirements of local law.

Under certain limited or exceptional circumstances, Ingram Micro may, as permitted or required by applicable laws and obligations, process Personal Data without providing notice or seeking consent. Such circumstances include the processing of personal data which is necessary for the conclusion or performance of a contract binding on the Data Subject, or as a legal requirement, or for the performance of a task carried out in the public interest or in the exercise of official authority, or in the legitimate interests of a natural or legal person, provided that the interests or the rights and freedoms of the data subject are not overriding.

Ingram Micro may also transfer or otherwise disclose Personal Data reasonably related to the sale, assignment, transfer or other disposition of all or part of any Ingram Micro business or undertaking, subject to and in accordance with applicable law.

EFFECTIVE DATE

This Policy is effective as of February 16, 2018.

As of the effective date this Policy replaces and supersedes any former Ingram Micro policy related to privacy or data protection.