Last Modified: May 18, 2018
Applicable Date: May 18, 2018

INGRAM CONTENT GROUP
DATA PRIVACY POLICY

SCOPE

This Data Privacy Policy ("Privacy Policy") applies to all Ingram Content Group[1] ("ICG") associates, vendors, contractors, and other third parties who have access to ICG systems or information ("Users"). Each User will comply with this Privacy Policy at all times.

From time to time, this policy may be updated or supplemented by the Information Technology, Human Resources, and/or Legal Departments.

PURPOSE

This Privacy Policy is intended to provide Users with the privacy principles under which ICG Processes personal information which may be received from the United States, countries belonging to the European Union ("EU"), United Kingdom, and/or other countries.

Any questions should be directed to ICG's privacy team at privacy@ingramcontent.com.

Definitions

Capitalized terms not otherwise defined in this policy will have the meanings as defined in the IT Security Management Policy.

"**Applicable Laws**" means (a) UK Data Protection Act 1998 and the GDPR; and (b) any other Data Protection Laws, to the extent such laws are applicable to ICG.

"**Associate Personal Data**" means the Personal Data of an ICG employee.

"**Data Protection Laws**" means the data protection or privacy laws of any country, state or other locale.

"**Data Subject**" means the individual who is the subject of Personal Data.

"**GDPR**" means EU General Data Protection Regulation 2016/679 as enacted into English law.

"Personally Identifiable Information" ("PII") means any information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. Further, PII is defined as: (1) information that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.), in conjunction

[1] The reference to ICG will include any Ingram Content Group entity now in existence or hereafter created or acquired including, without limitation, Ingram Content Group LLC, VitalSource Technologies LLC, Ingram Book Group LLC, ICG Ventures LLC, Ingram Fulfillment Services LLC, Ingram Publisher Services LLC, Book Network Int'l Limited, Ingram Library Services LLC, Ingram Hosting Holdings LLC, Tennessee Book Company LLC, Ingram Transportation Company LLC, Lightning Source LLC, Lightning Source UK Ltd., Lightning Source Australia Pty Limited, and Lightning Source Germany GmbH.

with other data elements which may allow indirect identification of an individual (e.g., a combination of gender, race, birth date, geographic indicator, and other descriptors); (2) information permitting the physical or online contacting of a specific individual; and (3) information containing Sensitive Data. PII can be maintained in paper, electronic or other media.

"Personal Data" will collectively refer to PII, Personal Information and/or Sensitive Data.

"Personal Information" means any information relating to an identified or identifiable living person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

"**Process"** (including "Processes", "Processing" and "Processed") of Personal Data means any operation or set of operations which is performed upon Personal Data, whether or not by automated means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure or dissemination, and erasure or destruction.

"**Sensitive Data**" is data that pertains to racial or ethnic origins, political or religious beliefs, or health or sex life.

POLICY

In Processing Personal Data, Users will comply with the following general principles.

Notice
Users will ensure a privacy notice is accessible to all Data Subjects, which will contain the purposes for which Personal Data is collected and used by ICG, in accordance with Applicable Laws. In certain situations, data is collected, Processed, stored and transported in an anonymous format. In that case, PII and Personal Data is not contained within the data, Data Subjects are not known by the data processors within ICG and no notice is required.

Any complaints or inquiries pertaining to ICG's collection, use, storage, or Processing of Personal Data should be directed to privacy@ingramcontent.com.

Choice
Where appropriate, ICG will provide each Data Subject the opportunity to opt out from allowing ICG to disclose his/her Personal Data to a third party or to use it for a purpose incompatible with the purpose for which it was originally collected or authorized. For Sensitive Data, affirmative choice (opt-in) must be given if the data is to be disclosed to a third party or used for a purpose other than its original purpose or the purpose authorized.

Accountability for Onward Transfer (to Third Parties)
ICG may transfer information to a third party providing systems or services on behalf of ICG, but only after the third party enters into a data privacy agreement ("DPA") with ICG or the ICG Legal Department has otherwise verified that the third party has reasonable controls in place to ensure that such data is Processed only for limited and specified purposes consistent with the consent provided by the Data Subject and as required by Applicable Laws.

Security

ICG takes reasonable precautions to protect Personal Data from loss, misuse, and unauthorized access, disclosure, alteration, and destruction. These precautions include password protections for online information systems and restricted access to Personal Data Processed by the Human Resources Department in accordance with the ICG IT Management Security Policy.

Personal Data Inquires

All inquiries from outside ICG, either written or verbal, concerning the identity, employment record, or performance of current or terminated associates will be referred, without exception, to the Human Resources Department for handling.

If the request is from a government agency, a Human Resources representative and/or the Legal Department will verify the credentials of the agency representative before releasing information about a current or former associate.

Children

Do not collect Personal Data from Data Subjects who are under the age of 13 unless approved by ICG Legal and IT. Once approved, a process must be in place where a parent's consent to the collection of any information of a child less than 18 years of age is required and which allows the parent to obtain a copy of the information their child has provided, or update the information, or to ask us to no longer use the information.

Sensitive Data

Sensitive Data may not be Processed at all, unless such data is collected solely for the purposes of Human Resources functions, the Processes have been reviewed and approved by the Ingram Industries Inc. AVP Information/Data Security and Privacy Officer. It is ICG's policy and practice not to collect or store Sensitive Data except for this limited purpose and then only as absolutely necessary as an employer.

Data Integrity and Purpose Limitation

Each User is expected to take reasonable steps to ensure that Personal Data within ICG systems is accurate, complete, and current. Where appropriate, the Data Subject may have access to review their information. All associates are asked to inform the Human Resources and Payroll Departments immediately in the event of changes to Personal Data.

The Personal Data collected from Data Subjects should be limited to the information that is relevant for the purposes of Processing and ICG will adhere to these principals for as long as it retains such information.

Transfer and Sharing of Associate Personal Data

Associate Personal Data may be stored in hard and electronic format locally within the office of the associate's employment as well as in the United States and other countries in which ICG, or an agent or contractor has a physical presence. Associate Personal Data may be shared in the normal course and scope of business between ICG entities worldwide to facilitate the uses described within this Privacy Policy. Associate Personal Data may also be shared with third party vendors (e.g. medical benefit providers, stock brokerages, retirement benefit providers, etc.) with whom ICG has chosen to outsource work, in order to facilitate the uses described herein. In the event data is provided to a third party, ICG will maintain its right to ownership of Personal Data to help ensure that adequate privacy precautions are utilized. ICG will at times be required to disclose Associate Personal Data to legal and regulatory authorities.

Access, Modification, and Removal of Associate Personal Data
Associates may have the ability to directly access and/or modify their Personal Data through ICG systems. Associates may also contact Human Resources for additional access and/or modification of their Personal Data. ICG will try to accommodate associate requests to remove non-essential Personal Data in accordance with Applicable Laws; however, the removal of essential Associate Personal Data may affect the associate's workplace responsibilities, as well as benefits. Personal Data that is necessary as part of an associate's employment will remain within ICG's systems so long as such retention complies with Applicable Laws.

Recourse, Enforcement and Liability
You may contact the Ingram Industries Inc. AVP, Information/Data Security and Privacy Officer at privacy@ingramcontent.com to register complaints, to submit access requests, or to address any other issues arising under this policy.

Verification
Ingram Industries Inc.'s AVP Information Data Security & Privacy Officer is responsible for conducting an annual assessment in order to verify that this Privacy Policy is published and implemented within ICG by its associates and that it conforms with the requirements of Applicable Laws. As part of this annual assessment, the Ingram Industries Inc. AVP, Information Data Security & Privacy Officer will also be responsible for confirming this Privacy Policy is accurate, comprehensive, completely implemented, and accessible to ICG associates.

Notification
You must immediately notify the ICG IT Security service desk (ext. 34357) and privacy@ingramcontent.com of any suspected or actual breach of this Privacy Policy, in accordance with the ICG IT Security Management Policy.

Disciplinary Action
Non-compliance with this policy may lead to disciplinary action, up to and including termination, in accordance with applicable laws. Failure to report known violations of the Privacy Policy to privacy@ingramcontent.com is considered a violation of this Privacy Policy.

Questions related to Personal Data
If you have any questions about this policy, the use of Personal Data, or your Personal Data you should contact a member of the privacy team at privacy@ingramcontent.comprivacy or your local Human Resources representative.