Effective December 2019

Important Privacy Information below:

MACMILLAN PRIVACY NOTICE for employees, applicants and contracted staff

All of the companies in the US Macmillan trade publishing and learning group, Holtzbrinck Publishing Holdings Limited Partnership; Holtzbrinck Publishers, LLC; Macmillan Publishing Group, LLC Bedford, Freeman and Worth Publishing Group, LLC; Hayden McNeil, LLC; Intellus, Inc.; and EBI Map-Works, LLC ("Macmillan"), are committed to protecting the privacy of our current and former employees, job applicants, and other people with whom we work as contracted staff. This Privacy Notice is designed to provide you with an overview of our practices regarding the personal information we collect, use, store and, when necessary, transfer, in connection with your application for employment, employment with us or with your work relationship with us through your employer.

1. The Macmillan HR Privacy Notice protects your personal information no matter how or where it is processed or stored. It also protects the personal information that we collect from you about others, such as information about references, your family members or beneficiaries.

2. All Macmillan employees whose responsibilities include collecting, processing or storing personal information are expected to assist in the protection of that information, by adhering to this Privacy Notice.

3. We collect, use, store and, when necessary, transfer, human resources and payroll information through automated and paper-based data processing systems. We have established routine processing functions, such as processing for regular payroll and benefits administration. We may also process your personal information on an occasional or *ad hoc* basis, such as when you apply for a new position or contact human resources for help. We have implemented an information security program that is reasonably designed to protect the confidentiality and security of your personal information.

4. In many cases, we collect personal information directly from you. We may also obtain information about you from third parties, such as background screening companies or benefits providers. We may collect information about you automatically when you use our computer systems, participate in our social media programs or swipe your access badge.

   Examples of the types of personal information that we may collect, use, store and, when necessary, transfer, include:

   - Contact and identification information (such as your name, address, and government-issued identification numbers),
   - Payroll, tax and benefits information,
   - Job-related information (such as work assignment details, travel and expense data and performance-related records),

- Educational and training information,
- Health information (collected, processed and stored primarily by our third-party vendors as needed for medical claims processing, leave of absence management, and similar purposes),
- Background screening data, such as reference checks, license verifications, and, subject to applicable law, criminal records checks which are typically provided to us by third parties who provide employment background screening services.
- Information needed for security, legal compliance and risk management. For example, if you are authorized to operate a company-owned vehicle, we will collect information regarding your driving permits and driving history and, from time to time, we will collect information on potential conflicts of interest that might impact your employment with us.
- Your image, which you may add to your company profile, or which may be collected by our security monitoring cameras or when you participate in public group discussions or video conferences, and
- Information related to your use of company technology (such as company email, system logs and access badge reader logs). We reserve the right, subject to applicable law, to access, inspect, disclose, and dispose of any electronic files, data, and messages created, stored, sent, or received through our systems as needed to protect our interests and satisfy our legal obligations.
- Personal emergency contact information (such as your personal phone number or email address) if you have voluntarily signed up for our IRIS emergency notification system.

5. We collect, use, store and, when necessary, transfer your personal information for customary human resources and business purposes, as permitted by law. We can summarize these purposes as follows:
    - Recruitment and staffing, including evaluation of skills and job placement, negotiation of compensation, benefits, relocation packages, re-employment, etc.
    - Determining your eligibility to work and assisting with work permits or visas, and conducting background checks, vetting and verification,
    - Staffing and job placement, including scheduling and absence management,
    - Administration of compensation, insurance and benefits programs, and (in some cases) diversity programs,
    - Time and expense management and other workplace administration tasks (such as managing Macmillan computers and other assets, providing communication and social media tools, facilitating relationships within Macmillan and with our clients and others, and offering community, alumni and retiree programs),
    - For occupational health and safety programs (including required reporting, disaster and pandemic planning, and incident management) as well as for company health and wellness programs, including offering onsite medical care and accommodating disabilities,
    - For talent and performance development, skills management and training, performance reviews (including client surveys), engagement surveys, recognition and reward programs and succession planning;
    - For HR support services, such as responding to inquiries, providing information and assistance, and resolving disputes,
    - For risk management, including employee and premises monitoring as set forth in other policies, and

- To respond to your requests, such as providing employment and income verification.

We may also process your personal information for everyday business purposes, such as:

- Identity and credential management, including identity verification and authentication, issuing ID card and badges, system administration and management of access credentials and processing data for information security and cybersecurity purposes by our security program technologies,
- Legal and regulatory compliance: all uses and disclosures of personal information that are required by law or for compliance with the Macmillan Code of Conduct and other policies and procedures, such as our fraud prevention programs, security and incident response programs, intellectual property protection programs, and corporate ethics and compliance hotlines,
- Corporate audit, analysis and consolidated reporting,
- To enforce our contracts and to protect Macmillan, our workers, our clients and their employees and the public against injury, theft, legal liability, fraud or abuse,
- Making back-up copies for business continuity and disaster recovery purposes, and
- To facilitate corporate governance, including mergers, acquisitions and divestitures.

6. We may disclose your personal information in the following circumstances:

   - To other Macmillan affiliates, including Holtzbrinck Publishing Holdings in the United States, which will handle your personal information in accordance with this Privacy Notice,
   - To our third-party vendors, which use the data only as permitted by our contracts with them, and to those companies that provide benefits and services to you,
   - When required by law, including to law enforcement agencies and courts in all of the countries where we operate,
   - When permitted by law, such as to our auditors and advisors, in connection with employment screening, employment verification or an internal investigation,
   - With your consent or as reasonably needed to protect your vital interests, such as in the event of an emergency or natural disaster, and
   - To an acquiring organization if we are involved in a sale or a transfer of some or all of our business.

7. Your personal information may be transferred to, stored at or processed in a location outside the country of your employment which may not have equivalent privacy or data protection laws. However, regardless of where your personal information is transferred, we will protect it in accordance with this Privacy Notice.

8. We will retain your personal information as needed for business and compliance purposes in accordance with our retention policies and applicable law.

9. You have shared responsibility with regard to the accuracy of your personal information. You may reasonably access and update your personal information and other personal information that you have provided and that you have on file with us (such as that of your family) by using the tools available on https://e22.ultipro.com.

10. If you have any questions about privacy or the security of your personal information, please contact your local Human Resources office. As part of our commitment to you, we will try to resolve any questions or concerns that you may have.

11. **Notice for Nevada residents:** Macmillan does not sell any Nevada personal information.

Important - Privacy Information for Macmillan Staff in the European Economic Area

Macmillan is providing this supplemental privacy notice to give individuals in the European Economic Area (EEA) the additional information required by the EU General Data Protection Regulation. These provisions, together with the statements in the above *MACMILLAN PRIVACY NOTICE for employees, applicants and contracted staff* explain our practices with regard to EEA personal data.

1. Information about Macmillan

All of the companies in the Macmillan trade publishing and learning group are committed to protecting the privacy of our current and former employees, job applicants, and other people with whom we work. Macmillan protects your personal data no matter how or where it is processed or stored. It also protects the personal data of others that we collect from you, such as information about your family members or beneficiaries.

This information is being provided by the Macmillan trade publishing and learning group for itself and its subsidiaries:

Holtzbrinck Publishing Holdings Limited Partnership
Holtzbrinck Publishers, LLC
Macmillan Publishing Group, LLC
Bedford, Freeman and Worth Publishing Group, LLC
Hayden McNeil, LLC
Intellus, Inc.
EBI MAP-Works, LLC

Macmillan is based in the United States. Our representative in the EEA is:

Macmillan Publishers International Limited
Company number: 02063302
Pan Macmillan
The Smithson
6 Briset Street
London, EC1M 5NR.

Att: Legal Department

Contact Point for inquiries:

Helaine Ohl, VP Global HR Director, Macmillan, 120 Broadway, 22nd Floor, New York, New York 10271 or email: Helaine.ohl@macmillan.com.

The Purposes and Legal Basis for Processing, including Legitimate Interests

Macmillan collects, uses, stores and, when necessary, transfers, human resources and payroll information through automated and paper-based data processing systems. We have established routine processing functions, such as processing for regular payroll and benefits administration. We also process personal data on an occasional or *ad hoc* basis, when changes occur.

Macmillan only processes your personal data when we have a legal basis for the processing. We will processes your personal data as needed:

- To fulfill our obligations under your employment contract (or as otherwise needed for customary human resources purposes), such as to pay you and provide benefits, and
- For closely-related purposes, such as work scheduling, talent development, performance reviews, asset management, corporate governance, occupational health and safety programs and legal compliance.

We may also process your personal data for the purposes of our legitimate interests, provided that such processing does not outweigh your rights and freedoms. In particular, we may process your personal data as needed to:

- Protect you, us or others from threats (such as security threats or fraud) and for auditing and verifying compliance with company policies,
- Comply with the laws that are applicable to us around the world,
- Enable or administer our business, such as for training and quality control, for purposes of conducting an investigation of alleged wrongdoing, customer service programs, equal opportunity programs, succession planning, and consolidated reporting, and
- Manage corporate transactions, such as mergers or acquisitions.

We may also process your personal data when requested to do by you, such as when you apply for a job with Macmillan or when you ask us to provide an employment verification to a third party.

2. Automated Decision-Making and Profiling

We will not use profiling techniques or make automated-decisions about you that may significantly affect you, unless (1) the decision is necessary as part of a contract that we have with you, (2) we have your explicit consent, or (3) we are required by law to use the technology.

4. When You are Required to Provide Personal Information to Macmillan

Providing personal data is necessary for us to have an employment relationship with you. In some cases, we are required by law to collect and report personal data about our employees to government agencies, such as for tax or occupational health purposes. If you have any questions about the personal data that Macmillan is collecting, please contact your local human resources manager at the address provided above.

5. Your Rights

Macmillan respects the rights of Macmillan Staff in European Economic Areas to access, correct and request erasure or restriction of your personal data as required by law. This means If you are a Macmillan staff member in the European Economic Areas:

- You generally have a right to know whether or not Macmillan maintains your personal data. If we do have your personal data, we will provide you with a copy (subject to the rights of others). If your information is incorrect or incomplete, you have the right to ask us to update it.

- You have the right to object to our processing of your personal data.

- You may also ask us to delete or restrict your personal data.

To exercise these rights, please contact your local human resources manager at the address provided above. Please understand that these rights are subject to some limitations, such as when we are processing or retaining data to comply with our own legal obligations.

If you believe that we have processed your Personal data in violation of applicable law, you may file a complaint at dataprivacy@macmillan.com or with a supervisory authority.

6. International Transfers

Your personal data may be transferred to, stored at or processed in the United States and other countries as needed to fulfill the employment relationship. However, regardless of where your personal data is transferred, we will protect it in accordance with the applicable EU data protection laws.

Please contact dataprivacy@macmillan.com if you would like more information about cross-border transfers or to obtain a copy of the Standard Contractual Clauses.

7. Data Retention

We will retain your personal data for as long as the information is needed for the purposes set forth in Section 2 above and for any additional period that may be required by law. If you are a Macmillan staff member in the European Economic Areas, you may request that we delete your personal data by contacting your local human resources manager at the address provided above. Unless we are required by law to retain your information, we will delete it within 30 days of your request.

Important - Privacy Information for Macmillan Staff in California

All of the companies in the US Macmillan trade publishing and learning group, Holtzbrinck Publishing Holdings Limited Partnership; Holtzbrinck Publishers, LLC; Macmillan Publishing Group, LLC Bedford, Freeman and Worth Publishing Group,

LLC; Hayden McNeil, LLC; Intellus, Inc.; and EBI Map-Works, LLC ("Macmillan") are committed to protecting the privacy and security of the personal information that is entrusted to us. This means we protect your personal information as well as the information of others that we collect from you, such as information about your family members or beneficiaries. We also comply with applicable privacy and security laws, including the California Consumer Privacy Act (CCPA).

The CCPA provides California residents with specific privacy rights. California consumers have rights to receive privacy notices, access and request deletion of their personal information. Although these rights do not yet apply to Californians in the context of their employee data, Californians are entitled to receive information about the purposes for which their personal information will be used from companies with whom they have an employment or contractual work relationship.

If you are a current Macmillan employee, you can use our HR Self Service tools at http://e22.ultipro.com to access and correct much of your Personal Information. You may also contact your local human resources manager for assistance. If you are an applicant, former employee or family member, please contact the Macmillan Privacy Office for assistance with privacy matters. The Privacy Office can be reached at: dataprivacy@macmillan.com.

3. General Purposes for Collecting, Using and Disclosing Personal Information

Macmillan collects personal information about its prospective, current, and former employees, contingent workers, and other individuals in the context of an employment or contractual work relationship (such as dependents). The categories of personal information, along with representative data elements, are listed in the chart below. We generally use, disclose and retain personal information for the following purposes:

(b) Personal Information pertaining prospective employees or contingent workers may be collected, use and shared for:
- Recruitment and staffing, including evaluation of skills and job placement,
- Hiring decisions, including negotiation of compensation, benefits, relocation packages, *etc.*,
- Determining an individual's eligibility to work and assisting with work permits or visas,
- Risk management, including background checks, vetting and verification, and
- Our Everyday Business Purposes (defined below)

(c) Personal Information pertaining to current employees and contractors may be collected, used and shared for:
- Staffing and job placement, including scheduling and absence management;
- Administration of compensation, insurance and benefits programs;
- Time and expense management and other workplace administration tasks (such as managing our computers and other assets, providing communication and social media tools, facilitating relationships within Macmillan and with our customers and others, and offering community programs);
- Diversity programs;
- Health and wellness programs, including offering onsite medical care and accommodating disabilities;
- Occupational health and safety programs (including required reporting, disaster and pandemic planning;
- incident management);
- Talent and performance development, skills management and training, performance reviews (including customer surveys), engagement surveys, and recognition and reward programs;
- Succession planning and tasks related to retention or reductions in force;
- HR support services, such as responding to inquiries, providing information and assistance, and resolving disputes;
- Risk management, including employee and premises monitoring;
- As requested by individuals, such as providing employment and income verification; and
- Everyday Business Purposes.

(d) Personal Information pertaining to former employees may be collected, use and shared for:
- Re-employment,
- Administration of compensation, insurance and benefits programs, including retiree and alumni programs,
- As requested by individuals, such as providing employment and income verification, and
- Everyday Business Purposes.

(e) Personal Information pertaining to individuals whose information is provided to Macmillan in the course of HR management (such as information pertaining to employees' family members, beneficiaries, dependents, emergency contacts, *etc.*) may be collected, use and shared for:
- Legal compliance (such as in connection with required screening programs),
- Administration of compensation and benefit programs,
- Workplace administration, such as maintenance of directories and to comply with child support orders or garnishments,
- To maintain emergency contact lists and similar records, and
- Everyday Business Purposes.

Everyday Business Purposes means the following purposes for which personal information may be collected, use and shared:
- Identity and credential management, including identity verification and authentication, issuing ID card and badges, system administration and management of access credentials,
- Security, loss prevention, information security and cybersecurity,
- Legal and regulatory compliance: all uses and disclosures of Personal Information that are required by law or for compliance with legally mandated policies and procedures, such as: anti-money laundering programs, security and incident response programs, intellectual property protection programs, and corporate ethics and compliance hotlines,
- Corporate audit, analysis and consolidated reporting,
- To enforce our contracts and to protect Macmillan, our workers, our clients and their employees and the public against injury, theft, legal liability, fraud or abuse, to people or property,
- As needed to de-identify the data or create aggregated datasets, such as for consolidating reporting, research or analytics,
- Making back-up copies for business continuity and disaster recovery purposes, and
- As needed to facilitate corporate governance, including mergers, acquisitions and divestitures.

4. Categories of Personal Information

This chart describes the categories of Personal Information that Macmillan collects in connection with its employment and contractual work relationships:

Category of PI and Representative Data Elements	**Additional Purposes for Collecting and Sharing the PI**
Contact Information • Full name, nicknames or previous names (such as maiden names) and preferred form of address • Mailing address • Email address • Telephone number • Mobile number	We use your Contact Information to communicate with you by mail, email, telephone or text about your employment, including sending you work schedule information, compensation and benefits communications, emergency notifications and other company information. Contact information is also used to help us identify you and personalize our communications, such as by using your preferred name. We also use the Contact Information you provided to us to communicate with your emergency contacts or beneficiaries about emergency notifications and other relevant company information.
Government-issued identification information numbers • Social security number • Driver's license number • Passport number • Other government-issued identifiers as may be needed for risk management or compliance (*e.g., if you are a licensed professional, we will collect your license number)*	We use your government-issued identification numbers: • To identify you and to maintain the integrity of our HR records, • To enable employment verification and background screening, such as reference checks, license verifications, and criminal records checks, subject to applicable law • To enable us to administer payroll and benefits programs and comply with applicable laws, such as reporting compensation to government agencies as required by law • For security and risk management, such as collecting driver's license data for employees who operate company

Category of PI and Representative Data Elements	Additional Purposes for Collecting and Sharing the PI
	automobiles, professional license verification, fraud prevention and similar purposes • For other customer business purposes, such as collecting passport data for employees who travel
Unique Identifiers • Company ID number • Benefits program identifiers • System identifiers (e.g., usernames or online credentials)	We use unique identifiers (including your employee ID number) for internal record-keeping and reporting, including for data matching and analytics, and to track your use of company programs and assets.
Relationship Information • Biographical data, resume or CV • Data from LinkedIn profiles and similar platforms • Education and degree information • Professional licenses, certifications and memberships and affiliations • Personal and professional skills and talents summaries (e.g., languages spoken, CPR certification status, community service participation), interests and hobbies • Diversity program data • Preferences related to religion *(such as kosher meal requests, holiday leave requests)* • Political opinion, PAC contribution data • Information provided for company professional networks (employee profile data), including alumni programs • Professional goals and interests • Personal pronouns	We use Relationship Information to help us understand our employees and for professional and personal development. We also use Relationship Information to foster a creative, diverse workforce, for coaching, and to guide our decisions about programs and services. For example, we tailor service programs to reflect our employees' commitment to different types of causes.
Transaction and Interaction Information • Employment dates, positions, reporting information • Time and attendance records • Leave and absence records • Payroll and benefits plan records • Travel and expense records • Training plan records • Performance records and reviews, disciplinary records • Re-employment eligibility	We use Transaction Information as needed to manage our relationship and run our human resources functions, such as scheduling work, providing payroll and benefits and managing the workplace.
Financial information • Bank account number and details • Company-issued payment card information, including transaction records • Personal payment card information, if provided for reimbursement	We use your financial information to facilitate compensation (such as for direct deposit and reimbursement of expenses) and for security and fraud prevention.
Health Information	We use your health information as needed to provide health and wellness programs, including health insurance programs, and for internal risk management and analytics.

Category of PI and Representative Data Elements	Additional Purposes for Collecting and Sharing the PI
• Medical information for job placement, drug testing and fitness to work examinations, accommodation of disabilities • Medical information for leave and absence management, emergency preparedness, and workers' compensation • Wellness program data • Information pertaining to enrollment and utilization of health and disability insurance programs • Information pertaining to provision of onsite medical care	
Online & Technical Information • Device information from devices connected to our networks • System logs, access logs and records of access attempts • Records from access control devices, such as badge readers • Records from technology monitoring programs, including suspicious activity alerts	We use the online and technical information for system administration, technology and asset management, information security and cybersecurity purposes. We may also use this information to evaluate compliance with company policies. For example, we may use access logs to verify employee attendance records.
Audio Visual Information • Photograph • Video images, videoconference records • CCTV recordings • Call center recordings and call monitoring records • Voicemails	We may use this information for general relationship purposes, such as call recordings used for training, coaching or quality control. We use CCTV recording for premises security purposes and loss prevention. We may also use this information to evaluate compliance with company policies. For example, we may use CCTV images to verify employee attendance records.
Inferred and Derived Information • Advancement potential and success scores • Flight risk and similar scores • Benefits program utilization scores	We use inferred and derived data to help tailor professional development programs. We analyze and aggregate data for workforce planning, such as to predict hiring needs in the future and to ensure pay and promotion equity
Children's data For Employee Beneficiaries and Dependents: *We collect children's data pertaining to children under 16 from the parents or guardians of the children. We do not collect any personal information directly from children under age 16.* • Child's name, date of birth and relationship to the employee • Benefit program eligibility and enrollment records For employees who are 16 or 17 years old: We collect the same information as we do for all other employees as specified in this grid.	For Employee Beneficiaries and Dependents: We use children's data to provide the benefits programs selected by the employee and for related purposes, such as dependent verification, fraud prevention and utilization reviews. For employees who are 16 or 17 years old: We use the collected data for the same purposes as set forth in this grid.
Compliance data • Employment eligibility verification records, background screening records, and other record maintained to demonstrate compliance with applicable laws, such as payroll tax laws, ADA, FMLA, ERISA *et al.*	We use compliance data for internal governance, corporate ethics programs, institutional risk management, reporting, demonstrating compliance and accountability externally, and as needed for litigation and defense of claims.

Category of PI and Representative Data Elements	Additional Purposes for Collecting and Sharing the PI
• Occupational safety records and worker's compensation program records • Records relating to internal investigations, including compliance hotline reports	