Effective April 2023

MACMILLAN PRIVACY NOTICE for employees and applicants

All of the companies in US Macmillan trade publishing and Macmillan Learning[1] (collectively "Macmillan"), are committed to protecting the privacy of our current and former employees and job applicants. 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 or employment with us.

- 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.

- 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.

- 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.

- 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, vaccine status 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

[1] Holtzbrinck Publishing Holdings Limited Partnership; Holtzbrinck Publishers, LLC; Macmillan Publishing Group, LLC Bedford, Freeman and Worth Publishing Group, LLC; Hayden McNeil, LLC; and EBI Map-Works, LLC.

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 AlertMedia emergency notification system.

- 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 and productivity, 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.

- We may disclose your personal information in the following circumstances:

  - To other Macmillan affiliates, 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.

- 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.
- We will retain your personal information as needed for business and compliance purposes in accordance with our retention policies and applicable law.
- You have shared responsibility with regard to the accuracy of your personal information. For employees: 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 http://macmillan.ultipro.com/. For job applicants, for access and update of your personal information, please see our Data Subject Access Request Portal.
- If you have any questions about privacy or the security of your personal information, please contact your Human Resources office at:

  For Macmillan Trade and Shared Services: Gracie Mercado, EVP, People and Culture, 120 Broadway, 24th Floor, New York, New York 10271, Gracie.Mercado@macmillan.com

  For Macmillan Learning: Kristin Peikert, SVP, HR, Comms and L& D, 10900 Stonelake Blvd, Ste 300, Austin, Texas 78759, Kristin.Peikert@macmillan.com

  For MPS: Wilson Steppe, Dir, Human Resources, [16365 James Madison Hwy, Gordonsville, VA 22942], wsteppe@mpsvirginia.com

- **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 and applicants* 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 and job applicants. 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
EBI MAP-Works, LLC

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

Macmillan Publishers International Limited
Company number: 02063302
Registered Office: Cromwell Place
Hampshire International Business Park
Lime Tree Way
Basingstoke, Hampshire, RG24 8YJ

Att: Legal Department

Our representative in the EEA is:

Macmillan Publishers International Limited 1st
Floor, The Liffey Trust Centre
117-126 Sheriff Street Upper
Dublin 1
D01 YC43

Att: Legal Department

For Macmillan Trade and Shared Services: Gracie Mercado, EVP, People and Culture, 120 Broadway, 24th Floor, New York, New York 10271 Gracie.Mercado@macmillan.com

For Macmillan Learning: Kristin Peikert, SVP, HR, Comms and L& D, 10900 Stonelake Blvd, Ste 300, Austin, Texas 78759, Kristin.Peikert@macmillan.com

For MPS: Wilson Steppe, Dir, Human Resources, 16365 James Madison Hwy, Gordonsville, VA 22942, wsteppe@mpsvirginia.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,

- 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 so 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.

3. 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.

4. 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.

5. 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.

6. 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. 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.

If you are or were a Macmillan staff member or applicant in the European Economic Areas,to exercise these rights, please visit our Data Subject Access Request Portal. 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.

7. 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.

Important Information for California Employees and Applicants

Macmillan is providing this privacy notice to give its California employees and job applicants, and other individuals in California whose personal information is collected for human resources purposes (such as dependents) the information required by the California Consumer Privacy Act and the California Privacy Rights Act.

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

We only collect, use and disclose personal information when we have a legal basis for the processing. We process your personal information (and information about others, such as your dependents) for customary human resources purposes, as needed to enable our relationship with you, to comply with law and for our legitimate interests. The categories of personal information, along with representative data elements, are listed in the chart below. We generally collect, use, and disclose personal information for the following purposes:

- Personal Information pertaining job applicants, prospective employees:
  - 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)

- Personal Information pertaining to current employees:
  - 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, and 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 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.

- 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.

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

Everyday Business Purposes means the following purposes for which any personal information may be collected, used and disclosed:
- 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 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.

2. Specific Categories of Personal Information

This chart describes the categories of Personal Information that we collect in connection with our work relationships.

Contact Information	
Representative Data Elements	• Your name, previous names and preferred names • Honorifics and titles • Mailing address • Email address • Home or mobile telephone numbers

Sources	We collect this information from you and from recruiters. We may also obtain your information from publicly available sources, such as LinkedIn. We may use a service provider to update or standardize mailing addresses.
Additional Purposes for Collecting	We use 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 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.
Categories of Recipients	We disclose contact information to our affiliates, service providers, contractors and others, such as couriers and telecommunications providers. We may also disclose your business contact information as needed for your job, such as providing your name and company contact information to customers, if you are a customer-facing employee.
Government-issued identification information numbers	
Representative Data Elements	● 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, your license number)*
Sources	We collect this information from you. We may also verify his information from third party sources, such as background screening companies and license issuers.
Additional Purposes for Collecting	We use government-issued identification numbers: ● To identify you and to maintain the integrity of our records, ● To enable employment verification and background screening, such as reference checks, license verifications, or 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 vehicles, professional license verification, fraud prevention and similar purposes, ● For other business purposes, such as collecting passport data and secure flight information for employees who travel.
Categories of Recipients	We disclose these identifiers to our affiliates, service providers, contractors as others, such as background screening companies, financial institutions, travel services companies and government agencies.
Biometric Identifiers	
Representative Data Elements	● Fingerprint, voice print, retina or iris image, or other unique physical representation ● Mathematical representation of your biometric identifier, such as the template maintained for comparison
Sources	We collect this information from you when you enroll in a biometric program. We may also collect the biometric identifiers automatically, such as through voice authentication tools are used by our call centers.
Additional Purposes for Collecting	We use biometric identifiers to help us identify and authenticate you, for security and similar purposes (such as tracking access in our facilities or for biometric timekeeping systems).
Categories of Recipients	We disclose biometric identifiers to our affiliates, service providers, contractors and others, such as cybersecurity firms. In some cases, biometric data may also be collected by other entities, such as landlords who own the buildings in which we have offices. These entities are responsible for their own privacy practices.
Other Unique Identifiers	

Representative Data Elements	● Company-issued ID number ● Benefits program identifiers ● System identifiers (e.g., usernames or online credentials)
Sources	We assign an employee number to you as part of onboarding. Benefits providers may also assign unique identification numbers to you. We collect device identifiers and other unique identifiers from your devices and from our websites, apps and platforms, which use cookies and other data collection technologies.
Additional Purposes for Collecting	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.
Categories of Recipients	We disclose the identifies to our affiliates, service providers, contractors and others, such as benefits providers and customers.
Employee Information	
Representative Data Elements	● 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 social and professional networks (employee profile data), including alumni programs ● Professional goals and interests
Sources	We collect this type of information from you and from publicly available sources, such as LinkedIn, background screening companies, former employers and third parties that verify your credentials.
Additional Purposes for Collecting	We use employee information to help us understand you and your skills, and for professional and personal development. We also use employee 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.
Categories of Recipients	We disclose employee information to our affiliates, service providers, contractors and others, such as customers. Biographical data of executives may be published as appropriate for their role. We disclose employee information to our others as needed to respect your preferences, such as requesting kosher or vegan meals for you, or to enable you to participate in internal and external affinity or community groups.
Employment Information	
Representative Data Elements	● Dates of employment, re-employment eligibility ● Position, Title, Reporting Information ● Work history information ● Documents, communications and work product generated in the course of your work, and metadata associated with your work activities ● Time and attendance, leave and absence records ● Payroll records ● Benefits and benefit plan records ● Travel and expense records ● Training plan records ● Performance records and reviews, commendations, disciplinary records
Sources	We collect this type of information from you and from others as you work. We receive this type of information from our service providers and contractors and from your coworkers, customers and others with whom you work.

	We may collect this information automatically when you access our facilities or use our networks and technology. For example, our learning management system automatically tracks the training programs you have been assigned or have taken.
Additional Purposes for Collecting	We use transaction information as needed to manage our business and run our human resources functions, such as scheduling work, providing payroll and benefits and managing the workplace and for compliance and reporting.
Categories of Recipients	We disclose transaction information to our affiliates, service providers, contractors and others, such as auditors, benefits providers, financial institutions, government agencies, or customers.
Financial information	
Representative Data Elements	● Bank account number and details ● Company-issued payment card information, including transaction records ● Personal payment card information, if provided for reimbursement
Sources	We collect this type of information from you and from our service providers, financial institutions and others, such as merchants with whom you interact using your company-issued payment card.
Additional Purposes for Collecting	We use financial information to facilitate compensation (such as for direct deposit and reimbursement of expenses), for financial management and for security and fraud prevention.
Categories of Recipients	We disclose financial information to our affiliates, service providers, contractors and others, such as auditors, financial institutions, or government agencies.
Health Information	
Representative Data Elements	● Medical information for job placement, including vaccination status, drug testing and fitness to work examinations, accommodation of disabilities ● Medical information for leave and absence management, workers' compensation programs, emergency preparedness programs ● Wellness program data ● Information pertaining to enrollment and utilization of health and disability insurance programs ● Information related to onsite medical care ● Information collected in connection with occupational safety programs, such as information about accidents and illness incurred at work
Sources	We collect this type of information from you and from our service providers, benefits and wellness program providers and others, such as healthcare providers that you instruct to disclose health data to us.
Additional Purposes for Collecting	We use your health information as needed to provide health and wellness programs, including health insurance programs, and for other employee benefits programs. We also use health information for internal risk management and analytics, such as in connection with our disabilities, workers' compensation and workplace safety programs.
Categories of Recipients	We disclose health information to our affiliates, service providers, contractors and others, such as healthcare providers, benefits providers, first responders (in the event of an emergency), or government agencies. We may also disclose health information to others if you require an accommodation, such as requesting an accommodation if we book travel for you.
Online & Technical Information,	
Representative Data Elements	● Data from devices that connect to our networks ● System logs, including access logs ● Records badge readers and other access control devices ● Records from technology monitoring programs, such as suspicious activity alerts
Sources	We collect these data elements automatically, when you access our facilities, systems or networks or when you interact with us online.

Additional Purposes for Collecting	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.
Categories of Recipients	We disclose this information to our affiliates, service providers, contractors and others, such as government agencies, or customers in connection with audits of us.
Audio Visual Information	
Representative Data Elements	• Photograph • Video images, videoconference records • CCTV recordings • Call center recordings and call monitoring records • Voicemails
Sources	We collect these data elements from you, such as when you submit a photo for your badge, and automatically, when you access our facilities, systems or networks, interact with us online, or participate in calls or meetings that are recorded.
Additional Purposes for Collecting	We may use audio visual information for general human resources purposes, such as call recordings used for training, coaching or quality control. We use photographs and 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.
Categories of Recipients	We disclose this information to our affiliates, service providers, contractors and others, such as government agencies, or customers in connection with audits of us.
IoT and Sensor Data	
Representative Data Elements	• Smart device records • Workplace sensors • Vehicle onboard device records
Sources	We collect these data elements automatically when you use connected devices or operated company vehicles.
Additional Purposes for Collecting	We use these data in connection with management of the devices, such as assessing usage data for device quality control and troubleshooting. We also use this data for compliance and risk management purposes, to help ensure safe operation of company vehicles.
Categories of Recipients	We disclose this information to our affiliates, service providers, contractors and others, such as government agencies. In some cases, data may be shared with the device or sensor manufacturer, for their internal quality and compliance purposes, pursuant to our contracts with them.
Inferred and Derived Information	
Representative Data Elements	• Advancement potential and success scores • Flight risk and similar scores • Benefits program utilization scores
Sources	We create inferred and derived data elements by analyzing other data, such as employment records or benefits utilization records.
Additional Purposes for Collecting	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, to ensure pay and promotion equity
Categories of Recipients	We disclose derived information to our affiliates, service providers, contractors and others, such as management consulting firms.
Precise Geolocation Data	
Representative Data	GPS data

Elements	
Sources	We collect geolocation data with your permission from your mobile device. We collect geolocation data automatically for GPS-equipment in company vehicles.
Additional Purposes for Collecting	We use geolocation data information to monitor company drivers and vehicles. We may also use this information to evaluate compliance with company policies. For example, we may use geolocation data to verify your trip reports and confirm compliance with driving rules.
Categories of Recipients	We disclose geolocation information to our affiliates, service providers, contractors and others, such as our insurers or law enforcement agents, if needed to recover lost or stolen property.
Children's Data	
Representative Data Elements	Child's name, date of birth, relationship to the employee
Sources	We collect children's data pertaining to children from the parents or guardians of the children. We do not collect any personal information directly from children under age 16.
Additional Purposes for Collecting	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.
Categories of Recipients	We disclose children's data to our affiliates, service providers, contractors and others, such as benefits providers or as needed for legal compliance.
Compliance Data	
Representative Data Elements	Employment eligibility verification records, background screening records, and other record maintained to demonstrate compliance with applicable laws, such as payroll tax laws, right to work laws and privacy laws Occupational safety records and worker's compensation program records Records relating to internal investigations, including compliance hotline reports Security clearance information Records of privacy and security incidents involving HR records, including any security breach notifications
Sources	We collect compliance data from you and from our providers, contractors, and others, such as screening companies' service, investigators, legal advisors and government agencies.
Additional Purposes for Collecting	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.
Categories of Recipients	We disclose compliance to our affiliates, service providers, contractors and others, such as auditors, investigators, legal services companies, government agencies and others as required by law.

3. Sensitive Personal Information

We collect, use and disclose sensitive personal information as needed for the purposes listed above. We do not use or disclose sensitive personal information about our workers or applicants other than as necessary for our human resources and compliance functions and for other legally authorized purposes. We do not process any sensitive personal information for the purpose of inferring characteristics about you.

Category of Sensitive Personal Information	Purposes for Use and Disclosure
Government-Issued Identification Numbers	We use and disclose Government-issued ID Numbers for identification, compensation and benefits programs, compliance and related purposes.
Account log-in credentials and financial account numbers (with password, access code or other credential that permits access to an account)	We use and disclose account access credentials and financial account numbers to ensure security of our systems, for compensation (such as making direct deposit payments), security, compliance and related purposes.

Precise Geolocation Data	We use and disclose Precise Geolocation data for management of company devices, vehicles and other assets, and for security, compliance and related purposes.
Information about racial or ethnic origin, religious or philosophical beliefs	We use and disclose these data elements in connection with our diversity and social governance programs and as otherwise authorized by you (such as if you participate in company community groups).
Information about union membership	We use and disclose these data elements in connection with labor relations programs and as otherwise authorized by you.
Contents of Mail, Email or Text Messages	Communications sent using company devices or over company networks are subject to Macmillan's Electronic Devices and Systems Policy, and contents of mail, email and texts may be accessed, used and disclosed by Macmillan for legitimate business purposes to the extent permitted by law.
Biometric Identifiers	We use and disclose Biometric Identifiers for access control, premises security, compliance and similar purposes.
Health Information	We use and disclose health information as described above, such as for employee health and benefits, occupational safety, compliance and related purposes.
Information about sex life or sexual orientation	We use and disclose these data elements as needed for employee benefits programs (such as providing benefits to same-sex partners), for diversity and social governance programs and as otherwise authorized by you (such as if you participate in our LGBTQ+ community groups).

4. Collection of Personal Information by Third Parties

In most cases, Macmillan only allows third parties to control the collection of personal information when those third parties are acting as a service provider or a contractor to us. These companies only retain, use and disclose your personal information in accordance with our contracts and applicable laws. However, we may allow third parties to control collection of personal information in the following situations:

- Certain employee benefits providers have direct relationships with you, such as for health insurance, employee assistance and financial services benefits. These companies handle your personal information in accordance with their own privacy notices and applicable law.

- We may pay for other benefits that you access by interacting directly with a third party, such as if you are authorized to use subscriptions or trade association memberships. In each case, the third party will provide you with its identification and privacy information prior to collecting your personal information.

- When you use Macmillan's websites and those provided by our service providers and partners, the websites may allow third party advertising partners to utilize cookies, web beacons or other technologies to deliver ads to you on our sites and to deliver our advertisements to you.

- Within our offices, we may allow third parties to collect information in connection with services that they offer directly to you. In each case the name of each third party will be provided to you prior to your interaction with the third party, and their collection of your personal information will only occur if you consent.

- We may engage professional consulting services or research firms to collect data for us. If you participate in a research program or coaching program, the third party will provide you its contact information and privacy notice before you are asked to provide any personal information to it.

5. Disclosures to Service Providers, Contractors and Third Parties

Macmillan does not sell personal information pertaining to our workers or share it with third parties for cross-contextual behavioral targeting. We may disclose your personal information in the following circumstances:

- Your personal information is shared within Macmillan (among our affiliates) as needed to achieve the purposes set forth above. Our affiliates are all bound by our inter-company agreements.

- We may disclose your personal information with our data processors, service providers and contractors. These companies may only use the data only as permitted by our contracts with them.
- If you enroll in our benefits programs, we may disclose your personal information to those companies that provide the benefits and services to you, such as companies that provide your health insurance or financial services. These companies will provide you with their own privacy statements.
- We disclose personal information when required by law, including to law enforcement agencies and courts in the countries where we operate.
- We may also disclosure your personal information as permitted by law, such as (i) with your consent, (ii) as reasonably needed to protect your vital interests, such as in the event of a medical emergency or natural disaster, (iii) to our auditors and advisors, such as in connection with any internal investigations or for legal matters, and (iv) to an acquiring organization if we are involved in a sale or a transfer of some or all of our business.

We may share limited elements of personal information with third parties as may be appropriate for your job. For example, if you are a customer-facing employee, we may share your name and business contact information with our customers as needed for them to be able to contact you for service.

6. Your California Privacy Rights

California law provides California residents with specific privacy rights:

- The right to know what personal information and sensitive personal information we collect
- The right to access your personal information
- The right to correct inaccurate personal information
- The right to request that we delete your personal information
- The right not to be retaliated against for exercising your privacy rights

If you are a current Macmillan employee, you can access and update your personal information by using the tools available on http://macmillan.ultipro.com/. To exercise your rights, please contact us through the Data Subject Access Request Portal. For Macmillan Learning, see here. For Macmillan Trade and Shared Services, see here.

If you would like to designate an agent, please send an email from your own email address to dataprivacy@macmillan.com indicating the name and email address of your agent. We will respond to that person's requests using both your email address and the agent's email address.

If you are exercising CPRA access or deletion rights on behalf of another person, please understand that we will need to verify your authority with the person you seek to represent.

We will not retaliate against you if you exercise your rights under CPRA.

In addition to the rights listed above, California law provides California residents with the right to know what categories of personal information are sold to third parties or shared with third parties for cross-contextual behavioral targeting and to opt-out the sales and sharing. Macmillan does not sell or share any human resources personal information. California law also provides California residents with the right to limit certain uses and disclosures of sensitive personal information. Macmillan only uses and discloses sensitive personal information for the purposes listed above, and you cannot limit these uses and disclosures. We do not process any sensitive personal information for the purpose of inferring characteristics about you.

7. Financial Incentives

Macmillan does not offer financial incentives for the collection or sale of personal information from employees.

8. Questions or Complaints

You may contact your local human resources manager or the Macmillan Privacy Office if you have any questions or complaints. The Privacy Office can be reached at dataprivacy@macmillan.com.