Warner Bros. Discovery Workforce Privacy Notice

Effective date: November 2026

1. OBJECTIVE

The Warner Bros. Discovery group and its affiliated companies ("**Warner Bros. Discovery**", "**we**", "**our**" or "**us**") are committed to responsible data protection practices.

This Privacy Notice explains how we collect, use, share and otherwise handle information about you as a member of our Workforce (as defined below).

If applicable privacy laws in your jurisdiction require even stricter standards for the handling of information about you than as described in this Privacy Notice, the relevant Warner Bros. Discovery entities will comply with those standards.

The Warner Bros. Discovery company that you work at or provide services for is known as a "Controller" of your information in connection with human resources management. This means that it makes decisions about how and why your information is used for this purpose. Where another Warner Bros. Discovery company or a third party is involved in workforce management, that company or third party may also be a Controller. You can learn more about Warner Bros. Discovery Controllers and affiliate companies by visiting our Controllers and Affiliates page.

2. DEFINITIONS

Contractors means any individual who is not employed by Warner Bros. Discovery and who is working for or on behalf of Warner Bros. Discovery, including contingent workers or contractors (whether directly or indirectly contracted), agency workers, freelancers, consultants, secondees and individuals on work experience or work shadowing placements.

Controller means the entity or entities that decides how and why Personal Information is Processed.

Personnel means our employees, regardless of classification or type and including full-time employees, temporary employees and interns. Solely for the purposes of this Privacy Notice, this definition also comprises all personnel referred to under the California Consumer Privacy Act (see Cal. Civ. Code § 1798.145(m)) for purposes of providing required notices. The definition of "Personnel" under this Privacy Notice is not intended to be co-extensive with the definition of "employee" or other personnel-related terms under any applicable employment or other law.

Personal Information means any data or information Processed by us that identifies, relates to, describes or is capable of being associated with, or may reasonably be linked, directly or indirectly, with an individual, including personal data and personal information as defined in the GDPR, UK GDPR, California Consumer Privacy Act or other applicable privacy law.

Processing, *Process* and *Processed* refer to the collection, use, sharing, deletion or other handling of Personal Information, whether or not by automated means.

Special categories of data means information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership; genetic data; biometric data Processed for the purpose of unique identification; and information concerning health, sex life or sexual orientation; and Personal Information relating to criminal convictions and offences or related security measures, as well as any other data types designated as special and/or sensitive under applicable privacy law.

Workforce means Contractors and Personnel.

3. TYPES AND SOURCES OF PERSONAL INFORMATION WE COLLECT AND PROCESS

We may collect some Personal Information from you directly. This may include, for example:

- **identity information** such as name, date of birth and title;
- **contact details** such as personal email address and telephone number;
- **financial and tax information** such as bank account details and tax status data;
- **recruitment information** such as CV, qualification details and education history;
- **government-issued identifiers** such as social security number and/or national ID number;
- **right-to-work information** such as residence and right-to-work status; and
- **information relating to family and next of kin,** such as their name and contact details (e.g. for administration of certain benefits). Please confirm that they are happy for their information to be provided to us before doing so.

We will tell you where you are required to provide Personal Information to us, such as where it is necessary for us to enter into or perform our contract of employment or engagement with you (e.g. regarding your right to work). You must report any changes to this Personal Information to us (particularly changes to your contact details and bank account number).

Provision of certain other Personal Information is optional. However, if you choose not to provide it, there may be some adverse consequences. For example, if you do not provide us with details of an emergency contact, we may not be able to contact them on your behalf in the event of an emergency.

We may also generate Personal Information about you. This may include, for example:

- **employment/engagement-related records,** such as your working hours and arrangements, job title, work history, professional memberships, annual leave and other absences, training records, work-related travel and expenses, and performance and corporate role information (such as your department, role level and reporting lines);
- **salary and billing information**, including regarding payroll and benefits;
- **compliance and risk management information**, such as details of any disciplinary or grievance procedures and, where applicable, the results of any background or security checks;

- **information about your use of our network, communications systems and devices**, including regarding your use of our computers and mobile devices (see section 6 of this Privacy Notice);
- **content of communications** (including emails, instant messages and other electronic communications) transmitted, received, created or stored using our systems; and
- **CCTV and other surveillance footage**, **access control records and location data** (including badging systems logs and entry and exit records).

We may collect Personal Information about you from other sources, such as:

- **government organizations, health providers and benefits providers**;
- **our business partners and service providers**, such as companies that provide us with payroll, training, background checks or travel services; and
- **publicly available sources,** such as posted on the internet or in newspapers, used for legally compliant vetting of our Workforce.

Personal Information collected from the sources described above may in some circumstances include special categories of data, such as:

- details of a health condition, illness or injury;
- information relating to occupational health and safety;
- information relating to race and ethnicity;
- biometric data Processed for the purpose of unique identification (in order to secure and monitor access and entry to some of our premises, and for health and safety purposes in any case of emergency);
- trade union membership; and
- information relating to criminal convictions and offences.

We may combine Personal Information that we obtain about you from other sources with the Personal Information that you provide to us directly or that we generate about you. We may use this combined Personal Information as described in this Privacy Notice.

4. PURPOSES FOR PROCESSING PERSONAL INFORMATION

We may Process Personal Information about our Workforce: (i) for the purposes described in this Privacy Notice; (ii) as further disclosed to you at the time of collection of the Personal Information; and (iii) as otherwise permitted under applicable law.

For example, we may Process Personal Information for the following purposes:

- **Human resources and Workforce management**
    - We may Process Personal Information to recruit, engage, support, develop, compensate and manage our Workforce. This may include:
        - interviewing, recruiting and hiring;

- conducting CV reviews, applicant vetting and background checks (where permitted by law), and providing support in applying for visa or work permits, if applicable;
- transfers, travel and relocations (including concerning family members, partners or next of kin where relevant). This may include immigration assistance and arranging and reimbursing business travel and entertainment expenses;
- arranging professional travel and hotel accommodation including relevant insurance, and conducting reviews required for high risk travel (such as travel to conflict zones);
- recording and managing terms and conditions of Workforce employment or engagement;
- providing Workforce with necessary hardware and software infrastructure;
- conducting Workforce surveys;
- facilitating internal communications, including company profiles and workforce directories;
- arranging, managing and monitoring attendance, including annual and sick leave, and reintegration back into the Workforce;
- investigating and resolving conflict of interest issues;
- conducting reviews of or investigating compliance with applicable laws and our policies;
- allocating, reviewing and issuing pay and other compensation;
- effecting deductions from payroll for tax and social security purposes, calculating statutory sick pay and maternity, paternity and parental pay, managing stock or share plans, and administering pension schemes;
- career management, including reviewing and appraising performance;
- training, development and succession management;
- offering coaching sessions, running live trainings, supporting career transition, and leadership development including award recognition;
- managing disciplinary and grievance procedures;
- administering benefits, including health insurance plans, pensions and family-friendly offerings;
- carrying out occupational health and safety assessments and necessary medical assessments, and offering and maintaining access to medical insurance, pension schemes and discount benefits for Workforce and their families;

- providing engagement opportunities, including discounts, loyalty or affinity programs, and access to sweepstakes, promotions, competitions, awards and company products and services;
- complying with applicable legal requirements, including anti-discrimination and health and safety requirements;
- monitoring Workforce diversity and implementing diversity initiatives;
- supporting social corporate responsibility activities, conducting analysis of Workforce diversity for DEI reporting, and running integration events and competitions;
- communicating with the Workforce and representatives including using personal communication channels in emergency situations; and
- publishing directories and organizing events.
- business and HR reporting and statistical analysis, including for headcount, resource allocation and business continuity;
- exit management, including succession management and providing references to third parties where requested;
- engaging with industry bodies and managing event attendance;

- **Business process execution and management**
  - We may Process Personal Information in order to run our business operations. This may include:
    - scheduling, recording, monitoring, evaluating and facilitating work engaged for Warner Bros. Discovery, the Workforce and other relevant third parties;
    - budgeting, planning, forecasting, project management and headcount and resource allocation;
    - auditing and monitoring compliance with our policies;
    - configuring and testing new, updated or upgraded systems, software and applications;
    - allocating, supporting and monitoring access to company facilities and systems;
    - managing company assets, including approving and liaising on artwork for licensed products;
    - tracking, collating and analyzing data and licensed business activities, including for financial purposes; and
    - operating and maintaining TV, theatrical and gaming accounting systems.
- **Safety, security and business continuity**

- We may Process Personal Information to ensure the safety and protection of our Workforce, resources, systems, consumers, customers, assets and communities. This may include:
  - managing occupational health and safety;
  - protecting the integrity, security and access to our resources, assets, systems, networks, information and facilities;
  - administering access rights to equipment, facilities, intellectual property and electronic platforms, and maintaining access logs;
  - monitoring compliance with information security policies, operating CCTV and other recording software, and managing badging systems;
  - providing systems, business information and data to relevant business divisions; and
  - operating disaster recovery, back-up, business continuity and alert systems.

- **Regulatory compliance**
  - We have various policies and procedures in place to comply with applicable laws and regulations. We may Process Personal Information in connection with these. This may include:
    - administering and providing training in relation to regulatory and compliance issues;
    - providing whistleblower protections where necessary to fulfil our compliance obligations (such as our obligations under U.S. legislation including the Sarbanes-Oxley Act and the Foreign Corrupt Practices Act);
    - conducting workplace compliance investigations and disciplinary or grievance procedures, including in relation to whistleblower and ethics reporting and conflicts of interest reviews;
    - monitoring ethical and regulatory compliance, including tracking and recording conflicts of interest;
    - implementing and monitoring compliance with our policies; and
    - cooperating with regulators, such as data protection authorities, tax authorities, law enforcement and sector-specific regulators.

Note that not all of the above purposes of Processing will necessarily be applied to the same extent or on the same terms to all Workforce, nor are they intended to be co-extensive with employment or other Workforce-related terms under any applicable employment or other laws.

We make available tested and approved enterprise-wide AI tools (such as Microsoft Copilot) for enhancing the productivity of our Workforce. If we introduce a new process or tool (including AI tools) that will result in the Processing of Personal Information for a purpose that is different from and is incompatible with the purpose for which the

Personal Information was collected, the Warner Bros. Discovery entity responsible for that new process or tool will, to the extent required by applicable law, inform the Workforce of the new process or tool and provide any required notices and/or privacy choices.

5. LEGAL BASIS FOR PROCESSING PERSONAL INFORMATION

In circumstances where the GDPR and/or UK GDPR applies to our Processing, we may Process Personal Information under the following legal bases:

- **Where necessary to enter into, administer and perform a contract with you (such as your contract of employment or engagement), manage our ongoing relationship with you, or provide services, resources and benefits.**
    - This may include, for example:
        - administration of insurance, payroll, benefits, leave and absence, compensation and authorized work-related travel and expenses;
        - Workforce and service provider management, such as onboarding and exit management and recording hours of work (including presence and absence);
        - providing access to medical insurance, pension schemes and other benefits offered by us or other providers, including management of employee transfers, travel and relocation and immigration assistance, if applicable; and
        - managing production-related rights and placement of credits, if applicable.
    - The categories of Personal Information that we may Process under this legal basis may include:
        - contact and identification information;
        - employment, engagement and recruitment information;
        - government-issued identifiers and right-to-work information;
        - compensation, payroll, billing, tax, banking and other financial information;
        - leave, attendance and scheduling information;
        - performance, training and career development information;
        - travel, relocation, immigration and expenses-related information;
        - information relating to dependents, beneficiaries, emergency contacts and next of kin;
        - health, occupational health and safety and benefits-related information;
        - trade union membership (where relevant and permitted by law); and
        - compliance and risk management information.

- **Where necessary to comply with legal and regulatory obligations**.
    - This may include, for example, obligations under applicable laws, regulations, court orders and industry standards, such as those relating to:
        - employment, labor, tax, statutory benefits and entitlements, social security and payroll reporting;
        - right to work and clearances;
        - statutory record-keeping and audit, accounting and regulatory reporting;
        - occupational health and safety and fitness-for-work assessments; and
        - responding to requests, inquiries and orders from governments, law enforcement, courts, regulatory bodies and other public authorities.
    - The categories of Personal Information that we may Process under this legal basis may include:
        - contact and identification information;
        - government-issued identifiers and right-to-work information;
        - employment, engagement and workforce management information;
        - compensation, payroll, billing, tax, banking and other financial information;
        - leave, attendance and absence information;
        - information relating to dependents, beneficiaries, emergency contacts and next of kin;
        - health, occupational health and safety and benefits-related information;
        - trade union membership (where relevant and permitted by law); and
        - compliance and risk management information.
- **Where necessary for the purposes of our legitimate interests or those of third parties**, provided that those interests are not overridden by your fundamental rights, freedoms or interests, and other than as required by law or to perform our contractual obligations.
    - Our legitimate interests may include:
        - **to develop and manage our Workforce effectively**, including training, performance management, career development, succession planning, professional recognition, communications and surveys, diversity and equality monitoring (in compliance with applicable law), and disciplinary and grievance processes;

- **to manage, plan and improve our business operations efficiently**, such as workforce planning, resource allocation, budgeting, business continuity, organizational restructuring, management reporting and international administration;
- **to protect our people, business and assets**, such as in connection with obtaining legal advice; establishing, exercising and defending legal claims and disputes; managing complaints and queries; conducting internal investigations and audits; and safeguarding confidential information and intellectual property;
- **to ensure compliance with our policies and standards**, including monitoring compliance, carrying out corporate social responsibility activities, providing Workforce engagement opportunities such as staff events and competitions, communicating with staff representatives (including work councils and trade unions);
- **to facilitate an actual or potential transaction**, such as a sale, merger or outsourcing that involves sharing Personal Information or where Personal Information forms part of the assets transferred;
- **to develop, commission, produce, publish, distribute, promote and commercialize our productions, games and other audio-visual content, if applicable**;
- **to store and archive our productions, games and other audio-visual content, if applicable**; and
- **to administer** access rights to our facilities, equipment, intellectual property and electronic platforms, and to maintain access logs and badging systems for security and compliance purposes.

- The categories of Personal Information that we may Process under this legal basis may include:
  - contact and identification information;
  - employment, engagement and workforce management information;
  - Workforce engagement information,
  - information relating to your use of our networks, communications systems and devices;
  - location data and physical security and access control information, including CCTV and access records;
  - diversity and inclusion information (where relevant and permitted by law);
  - information relating to actual and alleged criminal convictions and offences; and
  - compliance and risk management information.

- **Where necessary to prevent or detect unlawful acts.**
    - This may include:
        - performance of background checks (as relevant and applicable);
        - monitoring our premises (e.g. via CCTV), networks and systems; and
        - operating whistleblowing and fraud preventing practices (as applicable).
    - The categories of Personal Information that we may Process under this legal basis may include:
        - contact and identification information;
        - employment, engagement and workforce management information;
        - background check, screening and vetting information (where permitted by law);
        - information relating to your use of our networks, communications systems and devices;
        - location data and physical security and access control information, including CCTV and access records; and
        - compliance, investigations, whistleblowing and risk management information.
- **Where necessary to protect the vital interests of you or someone else in an emergency situation.**
    - The categories of Personal Information that we may Process under this legal basis may include:
        - contact and identification information;
        - employment and engagement information;
        - information relating to emergency contacts and next of kin;
        - location information, where relevant in an emergency; and
        - health and occupational health and safety information.
- **Where we have your consent.**
    - This may include:
        - to provide references to third parties at your request;
        - to carry out certain vetting and background checks where your consent is required by law; and
        - for Processing as described in any other consent we seek from you.

- The categories of Personal Information that we may Process under this legal basis may include:
  - contact and identification information;
  - employment and engagement information;
  - background check and vetting information; and
  - any other Personal Information covered by the specific consent obtained.

We only Process special category data where:

- we have your explicit consent;
- it is necessary for the purposes of complying with our legal obligations;
- it is necessary for carrying out our obligations or exercising our rights in relation to employment, social security or social protection law;
- it is necessary for establishing, exercising or defending legal claims;
- it is necessary for preventative or occupational medicine, assessment of working capacity or provision of healthcare; or
- it is otherwise required or permitted by applicable law.

Different jurisdictions recognize different legal bases for Processing Personal Information. To the extent that applicable laws do not recognize a legal basis referred to in this section, we may Process the Personal Information in reliance on another available basis, such as our legitimate interests where appropriate.

6. MONITORING

We carry out certain monitoring practices to help protect our people, business operations, information and assets. For example, we monitor our network and communications systems through automated tools such as network authentication and wireless connectivity hardware and software, anti-malware software, website and spam filtering software, security software for cloud-based applications, access and transaction logging, and mobile device management solutions. Our monitoring practices are carried out in accordance with applicable laws, workplace agreements and our policies and standards. Please refer to our Acceptable Use Policy and Mobile Device Policy for guidance on the appropriate use of our network, information and communication systems.

- **COMMUNICATIONS MONITORING**

Communications and information transmitted, received, created, stored, processed or recorded using our network, information and communications systems, devices, applications or technology resources are deemed to be business related and may be monitored, accessed, reviewed or analyzed by us in accordance with applicable law, workplace agreements (e.g. collective bargaining agreements) and our policies. This includes, for example, emails, documents, audio and video recordings, files, social media activity conducted through our systems, instant messaging communications, and interactions with AI tools made available to the Workforce, including via the use of

personal devices that access our network or communication systems. It may include any and all uses of devices such as computers, laptops and phones.

We reserve the right to monitor the Workforce's use of our technology resources to the maximum extent permitted by law and to review, use and disclose any information created, stored or transmitted on our IT systems for legitimate business purposes, including to respond to government investigations or in legal proceedings.

- **VIDEO AND ELECTRONIC MONITORING**

We conduct video monitoring (such as CCTV) and electronic monitoring activities (such as access control systems such as badge readers, and other technologies) in our premises and only electronic monitoring in remote workplaces). Monitoring may take place in common areas in our premises and facilities and vehicles used for business purposes, as indicated by signs on display.

As stated above, we may also monitor and access information created, transmitted, received or stored via our network, devices or systems. We use such monitoring activities for legitimate business purposes including maintaining the safety and security of people, premises, information and assets; protecting confidential information, intellectual property and company resources; preventing, detecting and investigating misconduct, fraud, security incidents and other unlawful incidents; and ensuring compliance with our legal obligations, contractual obligations and internal policies. Information generated through these monitoring activities may be collected on a routine basis and reviewed as necessary for these purposes. Warner Bros. Discovery may also implement additional monitoring measures or adjust existing monitoring practices where reasonably necessary for the purposes described above.

7. RETENTION OF PERSONAL INFORMATION

We hold Personal Information only for as long as is reasonably necessary for the purposes for which the Personal Information was collected as described in this Privacy Notice or as further disclosed to you. We may retain Personal Information for longer than this where required or permitted by applicable law, including:

- where we have your consent to use it for additional purposes;
- where we are permitted to retain it for artistic or journalistic purposes (such as in connection with a Warner Bros. Discovery production); or
- in line with standard legal limitation periods relating to the duration of your employment or engagement with us and for a certain period afterwards.

8. TRANSFERRING PERSONAL INFORMATION

We operate internationally and may store or Process Personal Information around the world and particularly in the United States, where Warner Bros. Discovery, Inc. is based. You can learn more about the countries in which we operate by visiting our Controllers and Affiliates page.

We implement appropriate measures to ensure that Personal Information is adequately protected in accordance with applicable privacy laws when we transfer Personal Information internationally, such as the European Commission's Standard Contractual Clauses, as applicable.

For further information about how we protect your Information when it is transferred outside of your country or region or to obtain a copy of said Standard Contractual Clauses, please submit a request by emailing wbdprivacy@wbd.com.

9. SHARING AND DISCLOSING PERSONAL INFORMATION

- *Within the Warner Bros. Discovery group*

All Warner Bros. Discovery entities are part of the Warner Bros. Discovery company group operating internationally. Certain Personal Information, such as corporate directory information and salary data, may be seen or accessed by authorized teams within the Warner Bros. Discovery company group, for example to help run our business and to comply with our legal and regulatory obligations.

- *Change of control*

In the event we go through a business transition such as a merger, acquisition, bankruptcy, reorganization, divestment, separation or sale of all or a portion of our assets, or a diligence process in connection with a potential business transaction, the Personal Information we hold may be disclosed, sold or transferred as part of that transaction. If such disclosure or transfer is subject to additional restrictions under applicable laws, we will comply with such restrictions.

- *With our service providers and professional advisors*

We may share Personal Information with authorized third parties that provide services to us (such as payroll providers, website operators, training and benefits providers, hotel and transport companies, insurers, security companies and providers of IT services including AI tools) and our professional advisors (such as lawyers, accountants and auditors).

- *With our partners*

We may share Personal Information with our business partners, such as co-producers, event partners, broadcasters, licensees, distributors and awards organizers.

- *With regulatory, legal, government and law enforcement bodies*

We may share Personal Information with third parties including law enforcement agencies and government authorities in certain circumstances, such as: (i) to investigate, prevent or take action regarding illegal activities or fraud; (ii) to comply with a request for Personal Information; (iii) to protect our people, business and rights, and the rights and safety of others; and (iv) as otherwise required or permitted by applicable law.

- *With other third parties*

We may share Personal Information with other third parties such as journalists who may interview our Executive Leadership, professional organizations, industry bodies, work councils, trade unions and emergency contacts and services.

- *With your consent*

In some circumstances, we may ask for your consent to share Personal Information with third parties, such as in order for your participation in voluntary Workforce social events.

10. COOKIES AND OTHER IDENTIFIERS

We may use cookies and certain other tracking technologies such as pixels and web beacons ("**Cookies**") on our websites, apps. Cookies are small pieces of script or code that are stored on your browser or device. We use Cookies that are essential to ensuring that our websites, apps and other digital products operate properly and securely, including enabling core functionality and recognizing you. Cookies also help us to understand how our websites, apps and other digital products are used, measure and improve their performance, personalize content, and help inform our business decisions. You have the option to accept, decline or customize Cookies at any time. However, please note that disabling or deleting certain Cookies may impact the availability or performance of our websites, apps and other digital products. You can also manage or limit Cookies by adjusting your browser settings in accordance with your browser instructions.

11. SECURITY MEASURES AND BREACHES

We aim to protect Personal Information by implementing and maintaining reasonable and proportionate organizational, technical and physical measures. Workforce also has an obligation to help protect our systems and information, and to comply with applicable policies and procedures concerning information security. For more information, please see the GICS document inventory to review our cybersecurity policies.

If you suspect that there has been a breach of our systems, your IT credentials, or any other circumstances that may compromise the security, integrity, confidentiality or availability of our IT resources or data, you must report your concerns immediately to the Security Operations Centre at +1 (404) 827-1900 or cybersecurity@wbd.com.

12. YOUR RIGHTS

Subject to applicable laws (such as the GDPR and UK GDPR, where applicable), you may have certain rights in relation to Personal Information we hold about you. This may include the right to:

- access Personal Information we hold about you;
- have inaccuracies or omissions corrected in Personal Information we hold about you;
- revoke your consent to us Processing Personal Information about you, where the Processing is based on your consent;
- in certain circumstances, object to us or restrict further Processing of Personal Information we hold about you or have us delete or otherwise remove the Personal Information;
- in certain circumstances, have the Personal Information we hold about you transmitted to another Controller (where technically feasible); and
- in certain circumstances, not be subject to wholly automated decision-making.

Additional information: Please also note the supplementary information for California residents and for Korea at section 17 and 18 of this Privacy Notice respectively.

If you would like to make a request regarding these rights, please consult the online Workforce intake form or email us at wbdprivacy@wbd.com. Please note that limitations apply.

If you are dissatisfied with how we have responded to your request or how we Process Personal Information, you may also have the right to complain to the data protection authority where you live, work or where you believe a breach in data protection law has occurred and to bring an action before the courts.

13. CONTACTING THE CONTROLLER

You can learn more about Warner Bros. Discovery Controllers and affiliate companies by visiting our Controllers and Affiliates page.

For Personnel, the Warner Bros. Discovery entity that employs is a Controller of your Personal Information.

For Contractors, the Warner Bros. Discovery entity that engages you or the organization that you work for is a Controller of your Personal Information.

For all Workforce, depending on the particular Processing activity, there may be more than one Controller. For example, where your Personal Information is shared with a parent company for business planning purposes, that parent company may also be a Controller in respect of that Processing.

Following a business transition or transaction, the Controller of your Personal Information may change. In these circumstances, entities which were previously Warner Bros. Discovery affiliate companies may no longer be part of our company group and may Process your Personal Information as a separate Controller. Where this is the case, the Processing will be handled in accordance with the privacy notice of the new Controller.

If you have questions about which entity is the Controller of your Personal Information, please contact us at wbdprivacy@wbd.com.

14. ETHICS AND COMPLIANCE CONTACT INFORMATION

The Warner Bros. Discovery Ethics and Compliance team is responsible for helping Workforce raise concerns about potential violations of our policies or applicable laws and regulations. This includes fraud, bribery and corruption, conflicts of interest, accounting or financial misconduct, misuse of company assets, retaliation and other unethical or illegal business conduct. Reporting channels made available by the team and proceedings resulting from submissions are confidential.

Contact details:

- ethics@wbd.com
- Ethics and Compliance Office, 230 Park Avenue South, 12th Floor, New York, NY 10003
- 24-hour Compliance Helpline: (800) 375-0288 or (800) 398-6395 (calls can be made anonymously)

15. UPDATES TO THIS PRIVACY NOTICE

We may update this Privacy Notice from time to time. We encourage you to periodically check back and review it. The date this Privacy Notice was last updated is provided above.

16. ACCESSIBILITY

We are committed to ensuring that our communications, including this Privacy Notice, are accessible to individuals with disabilities. To submit accessibility-related requests or to report barriers to accessibility, please contact us at the address, phone or email address above.

17. SUPPLEMENTARY INFORMATION FOR CALIFORNIA RESIDENTS ONLY

This supplementary information provides additional information for Workforce who are Californian residents. It applies to individuals covered by this Privacy Notice referred to under the California Consumer Privacy Act ("**CCPA**") for purposes of providing required notices.

This section applies only to information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with California residents or their households ("**California Information**"). It does not apply to information that has been "deidentified" or "aggregated consumer information" as defined by the CCPA.

CCPA Metrics

Regulations require us to disclose certain metrics for the previous calendar year regarding the requests by California residents. That information can be found by navigating to the CCPA Metrics Reporting page.

California Information We Collected

In the year before this section was last updated, we may have collected the following categories of California Information (each described further in section 3 of this Privacy Notice):

- **identifiers** such as name, postal address, phone number, date of birth, and online identifiers including cookie ID, IP address and MAC address;
- **internet or other electronic network activity information**, such as activities on our networks and systems like internet and email usage;
- **biometric information that is intended to establish identity**, such as a fingerprint, voiceprint or facial geometry mapping used for identification;
- **categories of Personal Information described in California Civil Code § 1798.80**, such as insurance policy numbers, financial account information and health insurance information;
- **characteristics of protected classifications under California or federal law**, such as gender, age and veteran status;
- **professional or employment-related information**, such as work history, training, job assignments and attendance;
- **education information**, such as schools attended, degrees or certifications obtained, or transcripts;
- **audio, electronic, visual, thermal, olfactory or similar information**, such as recorded training sessions and photographs for identification purposes;
- **geolocation data**, such as physical location based on badge scans;

- **California Sensitive Personal Information**, which includes information revealing social security, passport and other government identification numbers; account log-in and financial account numbers in combination with other information that may provide access to an account (such as log-in credentials for our information systems or direct deposit information); precise geolocation (such as through GPS trackers on company vehicles); racial or ethnic origin; citizenship or immigration status; union membership; religious or philosophical beliefs; contents of communications for which we are not the intended recipient (such as if you use our information systems for personal communications); health information; biometric information for the purposes of uniquely identifying an individual; and information collected and analyzed concerning sex life or sexual orientation; and
- **inferences drawn from any of the information identified above**, which may for example reflect preferences, characteristics, predispositions, behavior, attitude, abilities and aptitudes.

Purposes for Collecting California Information

We may have collected or used these categories of California Information for the business or commercial purposes described in section 4 of this Privacy Notice as well as

- Auditing compliance with the CCPA, other standards, and otherwise fulfilling our legal obligations
- Short-term, transient uses, such as verifying your identity when responding to a request

We do not use or disclose California Sensitive Personal Information for purposes that require an opt-out opportunity under the CCPA.

Sources of California Information

We may have obtained California Information from a variety of sources including:

- directly from you or devices you use; and
- indirectly, such as through:
    - third-party platforms and other technologies associated with our systems, facilities, or properties;
    - our affiliates, joint ventures and promotional and strategic partners;
    - other parties providing information about you (such as references and referrals) or our service providers and business partners involved in personnel matters like recruitment or background checks; and
    - publicly available sources.

Disclosures of California Information

In the year before this section was last updated, we may have disclosed the following categories of California Information to the following categories of third parties:

Category or Categories of California Information	**Categories of Parties**

Identifiers Internet or other electronic network activity Categories of Personal Information described in California Civil Code § 1798.80 Characteristics of protected classifications under California law Professional or employment-related information Education information Audio, electronic, visual, thermal, olfactory, or similar information Geolocation data California Sensitive Personal Information Inferences	• Our affiliates • Service providers that Process information on our behalf for the business purposes identified in this Privacy Notice • Professional services organizations, such as auditors or law firms • Background check services • Government agencies such as law enforcement • Other third parties to the extent necessary for purposes described in this Privacy Notice, such as our agents and representatives, successors in interest, and as reasonably necessary to meet our legal obligations
Biometric information	• Our affiliates • Service providers that Process information on our behalf for the business purposes identified in this Privacy Notice • Other third parties to the extent necessary for purposes described in this Privacy Notice, such as our agents and representatives, successors in interest, and as reasonably necessary to meet our legal obligations

In addition, as further described in section 9 of this Privacy Notice, we may disclose California Information as reasonably necessary to protect the rights, property or safety of Warner Bros. Discovery, our staff, and others; to protect against fraud or other unlawful or harmful activity; to comply with law or legal process; in response to requests from law enforcement or other government agencies; and in the event of a corporate reorganization, such as an actual or potential merger, or a divestiture, dissolution, or sale or transfer of some or all of our business assets, including as part of bankruptcy, liquidation, or similar proceeding.

We may have disclosed each of these categories of California Information for the purposes described in section 4 of this Privacy Notice.

Selling and Sharing

We do not "sell" or "share" (as defined in the CPPA) California Information of Workforce and have not done so in the prior 12 months. In this context, "share" means disclosing or making available for cross-context behavioural advertising. We do not knowingly "sell" or "share" California Information of Workforce we know to be under 16 years of age.

Data retention

We retain California Information for as long as is necessary for the purposes for which it was collected. This means that the retention periods will vary according to the type of California Information and the reason that we have this California Information. To determine the appropriate retention period for California Information, we consider the amount, nature, and sensitivity of the California Information, the potential risk of harm from unauthorized use or disclosure of California Information, the purposes for which we process California Information and whether we can achieve those purposes through other means, and the applicable legal requirements. Once the retention period expires and if not otherwise required to retain information by law, we will delete or de-identify California Information.

Your right to request access to California Information we collect and disclose about you

If you are a California resident, the CCPA grants you the right to request certain information about our practices with respect to California Information. In particular, you can request the following, subject to certain limitations or exceptions:

- the categories and specific pieces of your California Information that we've collected;
- the categories of sources from which we collected California Information;
- the business or commercial purposes for which we collected California Information;
- the categories of third parties to which we disclosed California Information and the categories of California Information disclosed to each

Your right to request the deletion of California Information

You may request that we delete the California Information we have collected from you. If an exception applies to your request, we will notify you.

Your right to request the correction of California Information

You may request that we correct inaccuracies in the California Information we have collected about you. We may follow up for documentation as needed, and we encourage you to make a good-faith effort to provide necessary information for us to evaluate your request at the time of your request.

How to exercise your California Rights

You may exercise your rights to request access to your California Information or deletion or correction of your California Information by submitting a request here. You can also contact us at Employee Connections at (US): 818-954-4636 or (US toll-free): 888-875-4455 for additional assistance and an agent will assist you with submitting a request.

When you submit a request, you must provide sufficient information to verify you are the person about whom we collected California Information (or the parent or authorized agent of that person, as explained below). We will ask you to provide an email address which we will use to contact you to confirm the request was not fraudulently submitted. Depending on the nature of your request, for your security and protection, we may need to verify your identity via a phone call. We may ask you to submit additional documentation to verify your identity, but we will only use this information for the purposes of verifying your identity for your request, security, or fraud-prevention, and not for any other purpose. That additional information will be deleted as soon as practical after verifying your identity.

If you are the parent of a child under 13 years of age, you may also submit a request on behalf of your child. To do so, we will ask you to provide your email address and your child's email address. We will then contact you at your email address to confirm the request was not fraudulently submitted. We will then need to verify your identity and relationship to your child. To do so, we may ask you to submit a signed form authorizing us to proceed with the request regarding your child's California Information. We may also ask you to provide additional documentation to verify your identity, but we will only use this information for the purpose of verifying your identity for your request, security, or fraud- prevention, and not for any other purpose. That additional information will be deleted as soon as practical after processing your request. Once we have confirmed your identity and authority to make a request on your child's behalf, we will start processing the req uest.

You may also designate an authorized agent to submit a request on your behalf. We will contact your authorized agent to confirm the request was not fraudulently submitted. We will then need to verify your authorized agent's identity and that they are authorized by you to make the request on your behalf. To do so, we may ask your authorized agent to submit a document of written permission authorizing your agent to act on your behalf, signed by both you and your agent. In the event your authorized agent is relying on a signed document of written permission from you, we may also need you to verify your identity and/or contact you directly to confirm permission to proceed with the request. Once we have confirmed your authorized agent's identity and authority to make a request on your behalf, we will start processing the request.

Your authorized agent can make a request by contacting us here or Employee Connections at (US): 818-954-4636 or (US toll-free): 888-875-4455.

You have the right not to be retaliated against if you exercise any of the rights explained in this section 17 of the Privacy Notice.

18. SUPPLEMENTARY INFORMATION FOR KOREA ONLY

This supplementary information provides additional information for individuals who are – or apply to become – part of the Workforce and whose Personal Information is protected under the Personal Information Protection Act of Korea ("**PIPA**").

This section applies only to individuals whose Personal Information is protected under PIPA and only to information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with those individuals ("**Korea Information**"). It does not apply to Personal Information that has been de-identified as provided by PIPA.

Korea Information Processed with your consent

We may Process the following Korea Information with your consent as set out below.

Korea Information	Purpose of Processing	Retention period
• name, address and contact details; • identity documentation (e.g. citizenship details, work permit); • financial information such as banking details and tax data; • educational background, background checks and references; • information about training, certifications, performance and disciplinary matters; • absence, holiday and related information; • access logs and CCTV footage; and • information about communications.	• administration of payroll, benefits, expenses and compensation; • Workforce management and supervision, including performance reviews, career development activities, maintaining absence records, taking decisions as to fitness for work, disciplinary matters; • administration and reporting, including to government authorities, law enforcement and regulatory bodies; • protecting our premises, information, people and assets, including intellectual property; and • assessment and enforcement of compliance with applicable laws and our standards and policies, including with respect to taxation and equal opportunities monitoring.	8 years from the date of termination of your employment or engagement with us (unless a longer retention period is required by applicable law).
• racial or ethnic information; • trade union membership; • health information; and • criminal convictions and related information.	• Maintaining sickness and absence records; • taking decisions as to fitness for work; • equal opportunities monitoring; and • physical security management.	
• passport information (including the passport number)	• administering employee insurance schemes and employee benefits.	

Korea Information Processed without your consent

We may Process the following Korea Information without your consent as set out below.

Legal basis	Purpose of Processing	Korea Information	Retention period
Article 15(1)(iv) of PIPA (where it is necessary to take measures at the request of a data subject in the course of performing a contract concluded with the data subject or concluding a contract).	To perform a contract with you and to enable you to perform any services for the purposes of your employment or engagement with us, including: • administration of payroll and compensation and expense management; • managing the Workforce and our service providers; • providing you access to medical insurance, pension schemes and other benefits; • rights management and placement of credits, if applicable; and • arranging professional travel and relevant insurance.	• contact details; • financial information; • recruitment information; • government-issued identifiers; • right-to-work information; • information relating to family and next of kin; • information about your employment or engagement for us; • salary or billing information; • annual leave and absence records; • training information; • compliance and risk management information; and • travel and expenses information (as described in further detail in section 3 of this Privacy Notice).	Until the contract is completed or as long as necessary to fulfill the contract, including post-contractual obligations. In most cases this will be 8 years from the date of termination of your employment or engagement with us.
Article 15(1)(vi) of PIPA (where it is necessary to attain the legitimate interests of a data controller,	• developing the Workforce; • planning our business, including succession	• contact details; • information about your employment or engagement with us;	For as long as necessary to fulfill the purposes set out on the left column (unless a longer period is

provided that such legitimate interests clearly outweigh the data subject's privacy rights).	planning, reorganization and restructuring; • developing, commissioning, producing, publishing, distributing, promoting and commercializing our productions, games and/or other audio-visual content; • storing and archiving our productions, games and/or other audio-visual content; • protecting our legitimate business interests and legal rights; • managing the performance and security of our equipment, facilities, intellectual property and electronic platforms in accordance with our policies; • ensuring the safety and protection of the Workforce and visitors; • carrying out communications and engagement activities; • publishing internal	• training information; • compliance and risk management information; • information about your use of our network, communications systems and devices; and • recruitment information (as described in further detail in section 3 of this Privacy Notice).	required by applicable laws).

	directories, charts and providing other internal communications tools; • analyzing and monitoring the diversity of the Workforce; • obtaining insurance and processing claims; • conducting Workforce surveys; and • recruitment and onboarding activities.		
Article 15(1)(ii) of PIPA (where special provisions exist in other statutes or it is unavoidable due to obligations under statutes or regulations). As required by applicable law, for example Article 127 of the Income Tax Act; Article 41 or the Labor Standard Act; or Article 48 of the Labor Standard Act.	To be determined by the relevant applicable law, but may include, for example: • withholding of income tax on employees' wages; • preparation and retention of the register of employees; and • preparation of the wage ledger.	To be determined by the relevant applicable law, but may include, for example: • resident registration number; • items included in the register of employees (e.g. name, date of birth, education and work history, etc.); and • items included in the wage ledger (e.g. matters serving as a basis for calculating wages and family allowances, salary data, etc.).	As long as necessary to comply with the relevant legal obligation.

Disclosure of Korea Information

We may disclose Korea Information as set out below.

Recipient	Purpose	Korea Information	Retention period
Our affiliates found at the Controllers and Affiliates page.	• human resources and Workforce management; • business process execution and management; • safety, security and business continuity; and • regulatory compliance (as described in further detail in section 4 of this Privacy Notice).	• contact details; • financial information; • recruitment information; • government-issued identifiers; • right-to-work information; • information relating to family and next of kin; • information about your employment or engagement with us; • salary or billing information; • annual leave and absence records; • training information; • compliance and risk management information; • information about your use of our network, communications systems and devices; and • travel and expenses information (as described in further detail in section 3 of this Privacy Notice).	As long as necessary to fulfill the purpose(s) listed in the column on the left (unless a longer retention period is required by applicable laws).

Kyobo Life	To provide insurance.	Unique identifying information, including passport number, name, national ID, salary information and information relating to dependents.	
DB Insurance	To provide insurance.	Unique identifying information, including national identity number and passport number.	
SafeGuard World International LLC	Payroll services.	Unique identifying information, including national identity number and passport number.	
Stone Global	Employee discount on the CNN licensed products.	Unique identifying information, including name and ID.	
Hunet	Online training courses for statutory mandatory trainings.	Unique identifying information, including name, email address and phone number.	
Pacific Prime CXA	Employee Flex Benefit Broker.	Unique identifying information, including national identity number and passport number, name, national ID, gender and information relating to dependents.	
Lockton	To provide insurance.	Unique identifying information, including national identity number and passport number.	
Hyundai Marine Insurance	To provide insurance.	Unique identifying information, including national identity number	

		and passport number.	
F&F	Employee discount on the Discovery Expedition licensed products.	Unique identifying information, including name and ID.	
Handle4U	Designated Driver Service.	Unique identifying information, including name, position, contact number, home address, and vehicle type.	
Optum	EAP provider.	Unique identifying information, including name or alias and confirmation of employment with us.	

We may provide the following Korea Information to third parties without your consent:

Legal basis	Recipient	Purpose	Korea Information
Article 15(1)(vi) and Article 17(1) of PIPA (where it is necessary to attain the legitimate interests of a data controller, provided that such legitimate interests clearly outweigh the data subject's privacy rights).	Relevant law enforcement and other government bodies.	To prevent unauthorized actions.	This will depend on the nature of the law enforcement or government request but could include: contact details; government-issued identifiers; information about your employment or engagement with us; and compliance and risk management information (as described in further detail in section 3 of the Privacy Notice).

Outsourcing of Processing of Korea Information

We may outsource the processing of your Korea Information as set out below.

Name of outsourced Processor	Outsourced Tasks
Aon Korea Inc.	Local Broker
Aon Hong Kong Limited	Regional contact for Aon

Tricor Korea Inc.	Local partner for SafeGuard World International LLC
Stone Global	L&M Licensee
Hunet	Online learning
Yeonsei Pure Internal Medicine Clinic	Private clinic for employee vaccination

International transfers (provision, outsourcing and storage) of Korea Information

We may perform international transfers of your Korea Information are specified below. If you do not want us to transfer your Korea Information overseas, you can refuse such transfer by requesting us to stop the international transfers of your Korea Information through one of the methods set out above. However, if you refuse the international transfers of your Korea Information, we may not be able to perform our obligations under the employment or engagement agreement. Legal basis for all the transfers listed below is Article 28-8(1)(iii) of PIPA, a separate consent of the data subject.

Recipient	Categories of Korea Information	Countries	Purpose	Retention period
Our affiliate entities.	• contact details; • financial information; • recruitment information; • government-issued identifiers; • right-to-work information; • information relating to family and next of kin; • information about your employment or engagement with us; • salary or billing information; • annual leave and absence records; • training information; • compliance and risk management information; • information about your use of our network, communications systems and devices; and	The countries where the Korea Information is to be transferred can be found on the Controllers and Affiliates page.	• Human resources and Workforce management; • business process execution and management; • safety, security and business continuity; and • regulatory compliance (as described in further detail in section 4 of this Privacy Notice).	As long as necessary to fulfil the purposes listed in the column on the left (unless a longer retention period is required by applicable laws).

	• travel and expenses information (as described in further detail in section 3 of the Privacy Notice).			
SafeGuard World International LLC	Unique identifying information, including national identity number and passport number.	Determined by the location of the recipient entity.	Payroll services.	As long as necessary to fulfil the purposes on the left (unless a longer retention period is required by applicable laws).
Stone Global	Name and ID.	Determined by the location of the recipient entity.	Employee discount on the CNN licensed products.	As long as necessary to fulfil the purposes on the left (unless a longer retention period is required by applicable laws).
Pacific Prime CXA	Unique identifying information, including national identity number, passport number, name, national ID, gender and information relating to dependents.	Determined by the location of the recipient entity.	Employee Flex Benefit Broker.	As long as necessary to fulfil the purposes listed on the left (unless a longer retention period is required by applicable laws).

Lockton	Unique identifying, information, including national identity number and passport number.	Determined by the location of the recipient entity.	To provide insurance.	As long as necessary to fulfil the purposes listed on the left (unless a longer retention period is required by applicable laws).
Optum	Unique identifying information, including national identity number and passport number.	Determined by the location of the recipient entity.	EAP Provider	As long as necessary to fulfil the purposes on the left (unless a longer retention period is required by applicable laws).
Aon Hong Kong Limited	Census files	Determined by the location of the recipient entity.	For regional contact for Aon.	As long as necessary to fulfil the purposes listed on the left (unless a longer retention period is required by applicable laws).

We may directly collect and Process your Korea Information from abroad. Countries where your Korea Information may be collected and Processed include Singapore, Hong Kong, the United Kingdom, and the United States.

Retention of Korea Information

We retain Korea Information for as long as necessary or for as long as we are required to retain Workforce Personal Information to comply with applicable laws and for the exercise or defense of legal claims. In most cases we retain Korea Information for a period of 8 years from the date of termination of your employment or engagement with us in order to comply with tax laws, for exercising or defending legal claims, as well as for future re-employment purposes.

The process and method of destroying your Korea Information after the retention periods are as follows.

- Process of destruction: we select the Korea Information to be destroyed and destroy it with the approval of the person responsible for Personal Information protection.
- Method of destruction: we destroy the Korea Information recorded and stored in the form of electronic files by using technical methods (e.g., low level format) to ensure that the records cannot be reproduced, while the Korea Information recorded and stored in the form of paper documents shall be shredded or incinerated.
- If we are required to retain your Korea Information by applicable legal obligations, we will retain the data only for the relevant retention period and the purposes required by such obligations.

Keeping Korea Information secure

We have implemented the following appropriate physical, technical, and organizational measures in line with legally required standards under PIPA to ensure the security of Korea Information:

- physical measures include access control to computer rooms and data storage rooms, etc.;
- technical measures include management of access rights to Korea Information Processing systems, installation of access control systems, encryption of Korea Information, installation and update of security programs; and
- administrative measures include the establishment and implementation of internal management plans, operation of dedicated organizations, and regular employee training.

Your rights

Your rights may also be exercised through your legal representatives or other duly authorized persons.