# Data Processing Addendum

This Data Processing Addendum applies where Service Provider Processes Personal Data as a processor or service provider on behalf of Company.

## 1. Definitions.

**1.1.** Capitalized terms that are not defined have the meanings assigned to them in Applicable Law or the Agreement. In the event of conflict or inconsistency between this Addendum or the Agreement, this Addendum shall govern. References to "Service Provider" include its Personnel.

**1.2.** Defined terms used in this Addendum have the meanings set forth below.

"**this Addendum**" means this Data Processing Addendum, which forms part of the Agreement.

**"Affiliate"** of a party means any entity that (as of the Effective Date, or thereafter at the applicable time) directly or indirectly now or hereafter controls, is controlled by, or is under common control with that party.

"**Agreement**" means the agreement between Company and Service Provider to which this Addendum is attached, as amended from time to time.

"**Applicable Law**" means all applicable laws, rules, regulations, rulings, judgments, directives, or other requirements of any governmental authority in any country or jurisdiction, as may be amended or otherwise revised from time to time and all applicable, current industry self-regulatory principles.

"**CCPA**" means the California Consumer Privacy Act as amended by the California Privacy Rights Act, and any related regulations.

"**Company**" means the NBCUniversal party to the Agreement.

"**Company Data"** means all data, including Company Personal Data, in any form, that is Processed by, or made available to, Service Provider or its Personnel in the course of providing Services under the Agreement, and all data regarding Company's use of the Services. Company Data includes Company's Confidential Information (which includes Company Personal Data, Company Content, and other Company Confidential Information) and any deliverables.

"**Company European Personal Data**" means all Company Personal Data to which Privacy Laws of the European Territories apply.

**"Company Personal Data"** means Personal Data that is Processed by or made available to, Service Provider in the course of providing Services under the Agreement.

"**Data Controller**", "**Data Processor**", "**Data Subject**", and "**Supervisory Authority**" shall have the meanings set out in the applicable Privacy Laws. Data Controller is inclusive of "**Business**" and "**Data Processor**" is inclusive of "**Service Provider**" as the terms are defined in the CCPA.

"**DPFs**" means collectively (i) the EU-U.S. Data Privacy Framework, (ii) the UK Extension to the EU-U.S. Data Privacy Framework, and (iii) the Swiss-US Data Privacy Framework.

"**Data Rights Request**" means a request by an individual to exercise their Privacy Law rights (regardless of whether the individual is actually entitled to that right).

"**European Territories**" means collectively (i) the European Economic Area ("**EEA**"), namely the European Union ("**EU**") Member States and Iceland, Liechtenstein and Norway, (ii) the United Kingdom ("**UK**") and (iii) Switzerland.

"**Order**" means a statement of work, order or other transactional document entered into by the parties pursuant to the Agreement.

"**Personal Data**" means any information that relates to an individual or household and that, alone or in combination with other information, can be used to identify, contact, or precisely locate an individual or household, or other information that constitutes "personal data" or "personal information" under Privacy Laws.

"**Personnel**" means, with respect to a party, that party's employees, Sub-processors, subcontractors, vendors, agents, officers, directors and other personnel.

"**Privacy Laws**" means all Applicable Laws and third-party platforms restrictions relating to the Processing of Company Personal Data, privacy and data security that may exist in any relevant jurisdiction.

"**Process**" (and any other tenses of the term "Process," such as "Processing") and words of similar nature mean using, accessing, storing, securing, sharing, disclosing, altering, destroying and deleting Personal Data and other actions as set forth in the applicable Privacy Laws.

"**SCCs**" means, in respect of Personal Data Processed by Service Provider for the benefit of NBCUniversal and/or its relevant Affiliates in: (a) the EEA and/or the Processing of EEA Personal Data, the unchanged, European Commission-

approved version of the standard contractual clauses in Commission Decision 2021/914/EU (as set out in https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en) (the "**EU SCCs**"); (b) the UK and/or the Processing of Company Personal Data to which Privacy Laws of the UK apply, the EU SCCs as modified by the International Data Transfer Addendum to the EU SCCs issued by the UK Information Commissioner under s119A(1) of the Data Protection Act 2018 ("**UK SCCs**"); and (c) Switzerland and/or processing Personal Data to which the Swiss Federal Act on Data Protection of 25 September 2020 and its implementing regulations ("FADP") apply, a version of the EU SCCs that is deemed to be modified as follows: references to "Regulation (EU) 2016/679" shall be interpreted as references to the FADP; references to specific Articles of "Regulation (EU) 2016/679" shall be replaced with the equivalent article or section of the FADP; references to "EU", "Union", "Member State" and "Member State law" shall be replaced with references to "Switzerland", or "Swiss law" ("**Swiss SCCs**").

**"Sell"** (and any other tenses of the term "Sell" such as "Selling") means selling, renting, releasing, disclosing, disseminating, making available, transferring, licensing, sublicensing or otherwise communicating orally, in writing, or by electronic or other means, an individual's Personal Data to a third party for monetary or other valuable consideration.

**"Sensitive Personal Data"** shall have the meaning set out in the applicable Privacy Laws and shall include, but not be limited to, "special categories of personal data" (as defined in the Privacy Laws of the EEA and UK) and "sensitive personal information" (as defined in applicable US Privacy Laws), as applicable.

"**Service Provider**" means the entity providing the Services.

"**Services**" means the services provided to Company and/or its Affiliates under the Agreement and any Orders.

"**Share**" (and any other tenses of the term "Share," such as "Sharing") shall have the meaning set out in the applicable Privacy Laws.

"**Sub-processor**" means any external party, including Service Provider's Affiliates and subcontractors, appointed by Service Provider to Process Company Personal Data. References to a Sub-processor include its Personnel.

"**Systems**" means websites, mobile or tablet sites, applications and other digital properties, services, platforms, software, servers, computers, hardware, firmware, middleware, networks, systems, workstations, data communications lines, routers, hubs, switches, magnetic, optical or electrical data storage devices, and all other information technology equipment.

"**Third Country**" means, (i) if the relevant Company entity is established in the EEA or Switzerland, a jurisdiction outside the EEA or Switzerland that has not been deemed adequate for data protection purposes by the European Commission, or (ii) if the relevant Company entity is established in the UK, a jurisdiction outside the UK that has not been deemed adequate for data protection purposes under UK law.

## 2. Roles and Responsibilities of the Parties.

**2.1. Independent Controllers.** Each Party ("**Controller Party**") acknowledges that it is an independent data controller with respect to Business Contact Data. "**Business Contact Data**" is Personal Data of the other Party's Personnel Processed by Controller Party for the purpose of facilitating the Services and maintaining the business relationship with the other Party. Each Party represents and warrants that it shall limit the use of Business Contact Data to such purposes.

**2.2. Service Provider as Data Processor.** The parties acknowledge that Company or its relevant Affiliates act as the Data Controller of the Company Personal Data Processed by Service Provider in its provision of the Services, and Service Provider acts as the Data Processor of such Company Personal Data. Service Provider acknowledges and agrees that between Service Provider and Company, Company owns all Company Data. In the event Company or its relevant Affiliates act as a Data Processor and Service Provider acts as the sub-processor, (a) each reference to Company or its Affiliates in their capacity as a Data Controller shall be interpreted to include the applicable Data Controller and (b) each reference to Service Provider as a Data Processor shall be interpreted to mean Service Provider's role as a sub-processor.

## 3. Processing and Disclosure of Company Personal Data.

**3.1.** Purpose of Processing Company Personal Data. Service Provider shall only Process Company Personal Data in accordance with Company's written instructions and the Processing details set forth in the Agreement or applicable Order, unless Service Provider is otherwise required by Applicable Law, in which case Service Provider shall (if legally possible) inform Company of that requirement before Processing the Company Personal Data. Company instructs Service Provider to Process Company Personal Data only to the extent necessary to perform the Services in accordance with the Agreement, this Addendum and the relevant Order. Service Provider shall notify Company immediately if it reasonably believes that any instruction given by Company is contrary to Privacy Law. Service Provider shall inform Company if it makes a determination that it cannot meet the requirements of this Addendum or a Privacy Law.

**3.2. Restrictions on Processing.** Service Provider shall not, without Company's prior written consent: (a) Process Company Personal Data for any independent purposes including outside the direct relationship with the parties, any purposes that are unrelated to providing the Services, or for the commercial benefit of Service Provider or any of Service Provider's other clients (to the extent permitted under Privacy Laws, detecting data security incidents, exercising and defending claims, and protecting against fraudulent or illegal activity are not considered commercial

benefits); (b) Sell or Share Company Personal Data; (c) to the extent Company Personal Data is anonymized or pseudonymized, re-identify, or attempt to do so with, such Company Personal Data, or any portions thereof; (d) delete or modify any Company Personal Data; (e) disclose Company Personal Data or any related summaries or reports to any third party or allow any third party to access it, including disclosure in any manner that would identify the methods, scope or scale of Company Personal Data or Company's use of the Services; or (f) combine Company Personal Data with or match Company Personal Data to Personal Data from its own or third parties' interactions with an individual. Service Provider certifies that it understands and will comply with the restrictions set forth in this Section 3. Service Provider shall comply with the obligations of the CCPA and provide at least the same level of privacy protection as required by the CCPA. Company shall have the right to take reasonable and appropriate steps to help ensure that Service Provider uses the Company Personal Data in a manner consistent with Company's obligations under Privacy Laws. Company shall have the right, upon notice, to take reasonable and appropriate steps to stop and remediate the unauthorized use of Company Personal Data. If Company directs Service Provider to cease or limit processing of Sensitive Personal Data Processed by Service Provider on behalf of Company, then it shall promptly do so, and cause its Personnel to do the same.

**3.3. Required Disclosures.** If Service Provider is required by Applicable Law to grant access to or otherwise transfer Company Personal Data to a third party (whether nationally or internationally), it shall:

(a) redirect the third party to request such information directly from Company;

(b) if permitted by Applicable Law, give Company as much prior notice as is reasonably possible;

(c) limit such access or transfer to the minimum required by Applicable Law; and

(d) provide Company with all reasonable assistance should Company choose to challenge such access or transfer.

**3.4. Processing Overview.** The categories of Company Personal Data to be Processed, the Processing activities to be performed, and the Sub-processors and Processing locations are set out in Annex 1 to this Addendum, the Agreement, or applicable Order.

**3.5. Data Processing Obligations.** Service Provider shall at no additional cost to Company:

(a) ensure that its Personnel are only granted access to Company Personal Data on a need-to-know basis; are bound by appropriate obligations of confidentiality; are appropriately supervised; and are provided with appropriate training in the care and handling of Company Personal Data;

(b) provide such information, cooperation and assistance to Company as Company may reasonably require to allow Company and its Affiliates to comply with their obligations under Privacy Laws including documentation needed to (i) demonstrate Service Provider's compliance with this Addendum; (ii) facilitate data protection impact assessments, (iii) address any enquiry, notice or investigation by a governmental authority, and (iv) facilitate the collection of required consents from data subjects;

(c) maintain written records of all categories of Processing activities carried out on behalf of Company containing the information prescribed in applicable Privacy Laws, and make such records available to Company on request; and

(d) notify Company promptly (and in any event within 2 business days) if Service Provider or its Personnel receive any inquiry or notice (including notice of investigation) from a governmental authority in relation to the Services provided under the Agreement.

**3.6. Data Rights Requests.** Service Provider will promptly (and in any event within 2 days' of Company's request) provide all information, co-operation or assistance as Company may reasonably require to fulfill the Data Rights Request. In addition, Service Provider will promptly inform Company of any Data Rights Requests regarding Company Personal Data that it receives directly from or on behalf of an individual. Service Provider shall either (a) provide an industry standard integration mechanism for the fulfillment of Data Rights Requests, or (b) integrate with a Data Rights Request fulfillment mechanism reasonably specified by Company.

**3.7. Sub-processors.** Service Provider is permitted to utilize the Sub-processors identified in the Agreement or applicable Order to Process Company Personal Data, and is permitted to appoint additional or replacement Sub-processors to process Company Personal Data, subject in all cases to Service Provider:

(a) carrying out adequate due diligence and monitoring to ensure that the Sub-processor will provide the level of protection for Company Personal Data that is required under this Addendum and, if applicable, the SCCs;

(b) providing at least 30 days' notice to Company of the identity and location of the proposed Sub-processor, a description of the intended processing to be carried out by the Sub-processor, the proposed data transfer mechanism (if applicable), and confirmation that adequate due diligence has been conducted on it, in order to give Company the opportunity to consider and object to such changes prior to the use of the proposed Sub-processor;

(c) complying with the requirements of Section 4.2(b) (Onward Transfers) and Section 4.3 (Transfers of Bulk U.S. Sensitive Personal Data) below; and

(d) requiring each of its permitted Sub-processors that Process Company Personal Data to enter into an agreement that imposes the same or substantially similar obligations that are in this Addendum.

If Service Provider identifies deficiencies in a Sub-processor's privacy or security controls, Service Provider shall maintain a record of such findings and ensure that such deficiencies are remediated within appropriate timeframes. Service Provider is liable to Company for the failure of Service Provider Personnel to comply with the Agreement to the same extent that Service Provider would have been had Service Provider failed to comply.

**3.8. Data Return and Deletion**. Unless (i) otherwise requested by Company in writing, or (ii) Service Provider is required to retain it under Applicable Law, Service Provider must return to Company or its designee, or at Company's written request, securely delete, destroy or render unreadable or undecipherable all Company Personal Data in the possession, custody or control of Service Provider, at the earlier of conclusion of the applicable Services, upon Service Provider no longer needing to Process Company Personal Data to provide the Services, or on written instruction from Company, and shall direct its Sub-processors to do the same. Service Provider shall promptly on Company's request certify that such Company Personal Data has been returned, deleted or destroyed.

## 4. Cross Border Data Transfer.

**4.1. Compliance with Cross-Border Data Transfer Requirements.** Service Provider shall, and shall ensure that its Sub-processors shall, comply with (and cooperate with Company to facilitate Company's and its Affiliates' compliance with) the requirements of applicable Privacy Laws, related to cross-border data transfer and/or data localization, such as the execution of data transfer agreements with Company or its Affiliates. If, for whatever reason, the transfer of Company Personal Data to Service Provider ceases to be lawful, the parties will work together in good faith to put in place alternative or supplementary measures to enable the compliant receipt of the Services. If Company and Service Provider are unable to agree on suitable measures to address the issue, then Company may (at its option) terminate the Agreement or reduce its scope.

**4.2. Transfers of Company Personal Data.**

(a) **SCCs.** If Service Provider (i) is established in a Third Country and Processes Company European Personal Data, or (ii) Processes Company European Personal Data at or from its facilities in a Third Country, the SCCs shall be incorporated by reference in this Addendum and shall apply between Company (and/or its relevant Affiliates in the European Territories), and Service Provider. The parties' roles and the information required by the Annexes to the SCCs shall be as set forth in Annex 1 to this Addendum. Nothing in this Addendum shall be construed to prevail over any conflicting clause of the SCCs. Each party acknowledges that it has had the opportunity to review the SCCs.

(b) **Onward Transfers.** Service Provider may transfer Company Personal Data to a third party or a location outside the country of origin, provided that Service Provider complies with the requirements of applicable Privacy Laws, including (where appropriate): transferring the data to a territory which has been approved as providing adequate protection under applicable Privacy Laws, participating in a valid cross-border data transfer mechanism under applicable Privacy Laws so as to provide appropriate safeguards for such data (e.g. the use of standard contractual clauses or binding corporate rules), and taking other steps required under applicable Privacy Laws such as performing third country risk assessments and applying supplementary measures to protect the data.

(c) **Data Privacy Frameworks.** "DPF Certifications" means self-certifications made by an eligible US company under each of the DPFs. If the parties wish to rely on Service Provider's DPF Certifications as a data transfer mechanism in place of the SCCs, the applicable DPF Certifications shall be identified in the Agreement or applicable Order. Company's acceptance of Service Provider's DPF Certifications in place of SCCs is made in reliance on the representations and warranties in Section 4.2(d), and is subject to the provisions of Section 4.2(e).

(d) **DPF Representations and Warranties.** Service Provider hereby represents and warrants that: (i) the Agreement or applicable Order accurately reflects its applicable DPF Certifications; (ii) Service Provider has not taken steps to voluntarily withdraw from any of these frameworks; and (iii) the scope of each of the self-certifications covers the services and processing activities that will be undertaken by Service Provider under this Agreement.

(e) **Use of SCCs if the DPFs are not a sufficient data transfer mechanism.** If (i) Service Provider ceases to hold a DPF Certification that Company or any of its Affiliates requires as a data transfer mechanism, or (ii) the scope of any of Service Provider's DPF Certifications ceases to cover the services and processing activities that are undertaken by Service Provider under this Agreement; or (iii) any of the DPF Certifications becomes invalid as a data transfer mechanism, the parties agree that the SCCs will be incorporated by reference into this Addendum in accordance with Section 4.2(a) above, and will be deemed to have been executed by the parties as at the date of the relevant event listed in this section.

**4.3. Transfers of Bulk U.S. Sensitive Personal Data.** Service Provider represents and warrants that Service Provider is not a Covered Person or Country of Concern, as set forth in Section 202.302 of the Department of Justice Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons, as amended from time to time (the "**DOJ Rule**") and will immediately notify Company if it foresees any circumstance or situation that would cause it to become such a Covered Person or Country of Concern. Service Provider shall not, without prior written consent from Company, transfer, disclose, sell, resell,

sublicense, or otherwise permit access to any bulk U.S. sensitive personal data to: (a) any individual or entity located in a Country of Concern; (b) any Covered Person; or (c) any third party that intends to, or is likely to, transfer the data to a Country of Concern or a Covered Person. All terms in this section have the definitions assigned to them under the DOJ Rule.

## 5. Data Security

**5.1. Security.** To protect Company Data, Service Provider shall (a) implement and maintain administrative, technical, physical, operational and organizational safeguards regarding security, continuation, backup, and disaster-recovery that are consistent with then-current, highest industry standards and practices and comply with Applicable Law; (b) only access and use Company Systems to the extent necessary to perform the Services. Service Provider shall regularly review the security measures it has implemented to protect Company Personal Data so as to ensure their appropriateness with regard to risk to the rights and freedoms of natural persons, which may evolve over time.

**5.2. Security Incident.** A "Security Incident" is any accidental, unlawful, or unauthorized access, use, damage, destruction, alteration, loss, or disclosure of Company Data (including by or on behalf of Service Provider or its Personnel, or by or through any of their Systems or the Services or deliverables). Service Provider will notify Company without undue delay and in any event within 48 hours of becoming aware of any Security Incident. Service Provider will (a) immediately investigate and take all reasonable steps to mitigate any potential damages and remediate the cause of the Security Incident; (b) provide Company with full details of the cause and impact of the Security Incident (including the categories and approximate number of Data Subjects affected and their country of residence and the categories and approximate number of records affected) and provide updates on any material developments or findings; (c) take all reasonable actions to prevent any similar reoccurrence; (d) cooperate with Company in its efforts to investigate, remediate and mitigate the effects of the Security Incident and fulfill its notification obligations; and (e) cooperate with Company with respect to any litigation and/or investigation by or against third parties in connection with the Security Incident. Service Provider must send notifications of Security Incidents to its main contact under the relevant Order, with a copy to cyber@nbcuni.com.

**5.3. Communications**. Company reserves the right to manage all communications concerning Company's or its Affiliates' involvement in any Security Incident with the affected individuals, governmental entities, the public and/or third parties. Service Provider shall not issue, publish or make available to any third party any statement, press release or any other communication that mentions Company or its Affiliates and concerns the Security Incident without Company's prior written approval. The foregoing provisions are not intended to restrict Service Provider's ability to communicate with its other customers or make legally required communications or notifications.

## 6. Data Protection Audits and Reviews.

**6.1.** Company shall have the right to audit Service Provider. Service Provider shall cooperate and provide accurate information. Company or its representatives may conduct such audits annually. If required by Applicable Law or if a Security Incident occurs, Company may conduct additional audits. The audits may include onsite visits. Service Provider shall permit Company to carry out ongoing manual reviews and automated scans for the purpose of monitoring Service Provider's compliance with this Addendum. If as a result of audits or reviews described in this Addendum, Company determines that Service Provider has failed to perform any of its obligations under this Addendum and/or the Agreement, then Service Provider shall, within ten (10) days develop a corrective action plan (including timeline), subject to Company's approval, and shall implement this plan accordingly. Service Provider shall certify in writing to Company that the corrective action plan has been completed upon request.

## 7. Miscellaneous

**7.1.** Service Provider shall:

(a) comply with all Privacy Laws in performing the Services and its other obligations under the Agreement;

(b) obtain all registrations and consents, and pay all fees, required by Privacy Laws for Service Provider's performance and/or Company's receipt of the Services and deliverables; and

(c) cause its Personnel working on Company's premises, or having access to Company Systems, to comply with all applicable Company regulations and policies. Service Provider shall take reasonable precautions with respect to the employment of and access given to its Personnel, including conducting background checks.

**7.2. Materiality and Injunction**. Without limitation to any other remedies, Company shall be entitled to seek equitable relief for any breach of this Addendum without posting any bond. Service Provider acknowledges that any breach by Service Provider of this Addendum constitutes a material breach of the Agreement.

# Annex 1

**Description of Transfer / Processing Overview**

This Annex 1 sets out the details of Processing referenced in Section 3.4 (Processing Overview) and Section 4.2(a) (SCCs) of this Addendum.

The Processing details below may be set forth in this Annex 1 or incorporated by reference from the Agreement or applicable Order. To the extent a Processing detail is addressed in the Agreement or applicable Order, it need not be repeated below.

1. **Categories of Data Subjects:** As described in the Agreement or applicable Order; if not specified there, **[***Service Provider to complete***].**
2. **Categories of Personal Data:** As described in the Agreement or applicable Order; if not specified there, **[***Service Provider to complete***].**
3. **Sensitive Personal Data (if any):** As described in the Agreement or applicable Order; if not specified there, **[***Service Provider to complee or state "None"***].**
4. **Applied Restrictions or Safeguards:** As described in the Agreement, applicable Order, or applicable security requirements. **[***Service Provider to complete or state "None"***]**
5. **Nature and Purpose of the Processing:** To provide the Services described in the Agreement and applicable Order**. [***Service Provider to complete or state "None"***]**
6. **Duration of Processing:** For the duration of the applicable Services, subject to the retention and deletion requirements of the Agreement and this Addendum. **[***Service Provider to complete or state "None"***]**
7. **Frequency of Transfer:** As necessary to provide the Services. **[***Service Provider to complete or state "None"***]**
8. **Permitted Sub-processors:** As identified in the Agreement, applicable Order, or Service Provider's applicable sub-processor list made available to Company. **[***Service Provider to complete or state "None"***]**
9. **Processing Locations:** As identified in the Agreement, applicable Order, or applicable sub-processor documentation. **[***Service Provider to complete or state "None"***]**
10. **Competent Supervisory Authority (where applicable):** As determined in accordance with the applicable SCCs. **[***Service Provider to complete or state "None"***]**