Last updated: March 2022

BBCS DATA PRIVACY GUIDELINES FOR THIRD PARTIES

1. Overview

Transparent and fair handling of personal data is essential to maintaining trust in BBC Studios' ("**BBCS**") brands. Any Licensee, Production Partner, Joint Venture partner, or other third party ("**BBCS Partner**") collecting data[1] in direct connection with a BBCS or BBC brand (the "**Brand Personal Data**") must follow the principles set out in this document. The intention is to maintain trust in our brands and protect individuals who are providing their data due to an association with those brands.

Ordinarily, BBC Studios does not act as a controller in respect of this data (except to the extent data is shared with BBC Studios for marketing purposes with the consent of individuals). Arrangements involving the processing of personal data on behalf of BBC Studios as a controller must be governed by a data processing agreement.

2. Use of Brand Personal Data

2.1. Brand Personal Data must, at all times, be processed in compliance with all applicable privacy and data protection legislation, codes of practice and industry regulations, including the General Data Protection Regulation (GDPR), the UK GDPR, UK Data Protection Act 2018 and Privacy & Electronic Communications Regulations (2003), to the extent these apply to the BBCS Partner as data controller or to the processing of personal data of individuals located in the UK or EU.

2.2. BBCS Partner shall be transparent about its collection and use of Brand Personal Data. This includes (i) clearly identifying BBCS Partner in any data collection forms/transactions (rather than the BBC brand or product/event name); and (ii) a Privacy Notice which identifies the data controller and details the purposes for processing personal data, general data handling practices and contact information, shall be made available whenever Brand Personal Data is collected.

2.3. BBCS Partner shall process the Brand Personal Data only in ways that are consistent with its Privacy Notice as notified to individuals at the time of collection.

2.4. Brand Personal Data shall not be shared with unrelated third parties (except contracted data processors) without the explicit consent of the individual, unless allowed and required by law. For the avoidance of doubt, the Brand Personal Data may not be sold or rented to other parties.

[1] Including, but not limited to, unique identifiers, usage and behaviour data and device data

2.5. Any online service provided in the UK must comply with the UK Age Appropriate Design Code. In circumstances where a product or service is aimed at, or likely to attract children[2], BBCS Partner shall confirm the age of individuals before collecting any personal data or allowing someone to submit content. Children under the age of 16 should not be allowed to contribute content publicly nor should others be allowed to send them direct messages unless the content is pre-moderated. BBCS Partner shall obtain consent from their legal guardian in accordance with local regulatory guidance, and in any case for all children under the age of 13.

2.6. If Brand Personal Data is processed by (or otherwise shared with) a third party, BBCS Partner shall: (i) ensure the personal data will be kept secure; and (ii) enter into a written agreement with the third party detailing how the Brand Personal Data shall be handled in accordance with applicable data privacy law.

2.7. Brand Personal Data that has been collected or processed within the UK or European Economic Area (EEA) may only be transferred to countries located outside the UK/EEA which ensure an adequate level of protection as defined by the UK Government/European Commission or where adequacy is otherwise assured (for example via the UK/EU Standard Contractual Clauses).

2.8. BBCS Partner shall ensure that Brand Personal Data is only retained for as long as it is required to fulfil the purpose(s) for which it was collected and as required and allowed by law and shall implement processes to ensure the secure destruction of the data once there is no longer a lawful reason to retain it.

3. Online Privacy – Cookie Compliance

3.1. BBCS Partner shall comply with any legal obligations relating to the use of cookies and other online tracking technologies and applicable regulatory guidance issued in the countries where the service is available.

3.2. BBCS Partner shall publish a Cookies Notice (usually achieved via a cookie banner or 'pop-up') that details how such technologies are used on the site/app and the specifics of each type deployed. This notice shall be accessible on an ongoing basis via a permanent link in the footer of the service.

3.3. In the UK and EU, and any other country with similar legal requirements, BBCS Partner shall:

3.3.1. Provide a notice to all first-time visitors informing them of the use of cookie and/or tracking technologies and including a link to the full Cookies Notice;

3.3.2. Implement a technical solution to obtain the consent of users for the use of any non-essential cookies before any such cookies are stored or accessed on the users device. Due to the complexity and expense in building such a mechanism, it is recommended

[2] Persons under the age of 16, or as defined by local law

that BBCS Partner should purchase a Cookie Management Platform from a recognised specialist provider;

3.3.3. Ensure that all cookies are appropriately categorised in-line with current regulatory guidance; and

3.3.4. Prior to launching an online service, BBCS Partner shall ensure their chosen cookie consent management platform is correctly implemented and rigorously tested to verify that non-essential cookies are not deployed prior to consent being given.

3.3.5. BBCS reserves the right to verify compliance of the online service prior to launch and during the license period.

4. Marketing

4.1. Electronic direct marketing communications shall be sent only to individuals who have indicated their consent to receiving them, unless otherwise allowed by law and agreed with BBCS.

4.2. If BBCS Partner has an agreement with BBCS to obtain consent for BBCS to send marketing communications, it shall do so using a separate statement which names BBCS as the relevant controller and provides a link to the BBCS privacy policy.

4.3. Any marketing communications sent in connection with a BBCS brand must additionally comply with applicable marketing and/or advertising regulations and codes of practice.

5. Consulting with BBCS

5.1. Prior to the collection or use of Brand Personal Data, BBCS shall be notified of the categories of personal data to be collected and the purpose(s) for which they shall be processed.

5.2. If required, BBCS shall be supplied with copies of any consumer facing notices (including the Privacy Policy), marketing statements, and data collection forms before they are published and, in respect of notices specifically relating to BBCS, shall require the prior written approval of BBCS.

5.3. BBCS Partner shall inform BBCS, within a reasonable timeframe, if it receives any complaint, notice or communication which relates directly or indirectly to its processing of the Brand Personal Data and shall provide BBCS with the opportunity to review any response before it is sent.

5.4. BBCS Partner shall notify BBCS in writing immediately upon becoming aware of any material breach by BBCS Partner or its agents of these Guidelines or any applicable privacy and data protection legislation, regulations or codes of practice.

6. Information Security

6.1. BBCS Partner and its sub-processors shall process and store Brand Personal Data securely at all times and maintain IT systems used to process Brand Personal Data in a secure manner and in accordance with industry best practice, such as ISO 27001/2 and PCI DSS. In particular:

i. An appropriate level of encryption shall be applied to data whilst in transit and, as necessary, at rest (for example, where sensitive data is collected) using the latest industry standard encryption methodology (a minimum of TLS v1.2 or AES 256);

ii. Firewalls, virus scanning and monitoring shall be deployed on computer systems and networks used to process the data with any suspicious activity investigated and remediation action taken as necessary and implement immutable logging with a retention of 90 days minimum; and

iii. IT systems and networks shall be subject to penetration and vulnerability testing at intervals agreed with BBCS. Such testing is to be carried out as appropriate by BBCS Partner and the findings of internal testing shall be made available to BBCS security personnel and where applicable remediation plans put in place.

6.2. Without prejudice to 4.4, BBCS Partner shall notify BBCS (via email to dataincidents@bbc.com) without undue delay if it becomes aware of any unauthorised or unlawful processing, loss of, damage to or destruction of the Brand Personal Data ("Data Security Breach") and thereafter keep BBCS fully informed in writing with full details of the breach and provide BBCS with a full report of any investigation into the same.

6.3. BBCS Partner shall, at its own cost and following consultation with BBCS, take all reasonable steps necessary to mitigate the consequences of a Data Security Breach or (if applicable) to protect against a threatened Breach.

6.4. In the event of repeated Data Security Breaches, at the request of BBCS and at BBCS Partner's cost, BBCS Partner shall provide independent assurance of the resilience and security of the BBCS Partner's systems, process and personnel used to process the Brand Personal Data by means of an audit (for the benefit of BBCS) of BBCS Partner's systems, processes and personnel, to be undertaken by a reputable third party audit firm with appropriate expertise.

6.5. The BBCS Partner shall, promptly at its cost, carry out any corrective action plans recommended following an audit pursuant to 6.4 that are necessary to ensure compliance by BBCS Partner with these Guidelines.