Bright Horizons Family Solutions: DATA PROTECTION TERMS

1. The Data Protection Terms ("DP Terms") cover information security and privacy requirements applicable to the Services and are incorporated into the Agreement. The DP Terms supersede any prior agreement between the parties relating to information security and privacy. Unless otherwise provided expressly in the DP Terms or defined in Applicable Privacy Laws, terms used in the DP Terms shall have the meanings ascribed to them in the Agreement. If there is a conflict between the terms and conditions of the Agreement and the DP Terms, the DP Terms shall prevail.

Section A – Role of the Parties

2. The parties acknowledge and agree that depending upon the Services:
   - **2.1.** Bright Horizons Processes Client Personal Information as a Processor on behalf of Client as set out in Annex C.
   - **2.2.** Bright Horizons Processes Bright Horizons Personal Information as an independent Controller. Details of such Processing are outlined in its Global Consumer Privacy Notice at https://www.brighthorizons.com/Privacy.
   - **2.3.** When Bright Horizons shares Bright Horizons Personal Information with Client, it does so as an independent Controller to Controller.

3. The parties acknowledge and agree that each party shall be independent Controllers of the other party's Business Contact Information.

Section B – General Terms Applying to both Parties

4. In relation to Personal Information, each party shall (and shall require any parties it authorises to Process Personal Information to) comply with Applicable Privacy Laws and render such assistance as the other party may reasonably request to comply with Applicable Privacy Laws. For the avoidance of doubt, a reasonable request includes (but is not limited to) providing information necessary to enable the Controller to conduct a privacy / data protection risk assessment required by Applicable Privacy Laws.

5. In relation to any person it authorises to Process Personal Information, each party shall ensure such person is subject either to an executed written contract to keep Personal Information confidential or a legal obligation of confidentiality.

6. Any information provided by a party to fulfil an obligation under the DP Terms shall be treated as confidential by the receiving party.

7. In relation to Business Contact Information, each party agrees that the other party can use its Business Contact Information only for the purpose of allowing each party to perform or receive benefits under the Agreement, such as but not limited to contract/Services management and invoicing.

Section C –Client Personal Information

8. Processing instructions.
   - **8.1.** Bright Horizons shall Process Client Personal Information only:

8.1.1. as reasonably necessary and proportionate to deliver the Services and/or fulfil its obligations under the Agreement, including managing or administering the Services;

8.1.2. to comply with other written instructions provided by or on behalf of Client where such instructions are consistent with the terms of the Agreement or as agreed by both parties in writing; or

8.1.3. as required by an Applicable Law to which Bright Horizons is subject. If allowed under Applicable Law, Bright Horizons shall inform Client of the requirement before Processing, giving Client an opportunity to object or challenge the requirement directly.

8.2. Without prejudice to the generality of the above, Bright Horizons shall not:

8.2.1. attempt to or re-identify any previously aggregated, deidentified, or anonymized Client Personal Information except as specifically instructed in writing by the Client;

8.2.2. Sell or Share any Client Personal Information; or

8.2.3. subject to clause 8.3, combine Client Personal Information that Bright Horizons receives from (or on behalf of the Client) with Personal Information that it (i) receives from (or on behalf of another person or persons), or (ii) collects from its own interaction with the Data Subject.

8.3. Bright Horizons may combine Client Personal Information with other Personal Information as necessary to provide the Services.

9. Retention of Client Personal Information.

9.1. Bright Horizons may retain copies of Client Personal Information only as follows:

9.1.1. for the Processing duration identified in Annex C; or

9.1.2. to establish, exercise or defend legal claims.

9.2. Subject to clause 9.1, at Client's written request, Bright Horizons shall cease Processing Client Personal Information by deleting or returning it (including any copies) at the end of the Agreement unless Applicable Laws require retention of it.

9.3. The DP Terms shall continue to apply during any retention period.

10. Requests and Complaints.

10.1. In relation to Client Personal Information, without undue delay and within three (3) business days or such shorter period as reasonably required for Client to comply with Applicable Privacy Laws, Bright Horizons shall notify Client of:

10.1.1. requests from Data Subjects exercising their rights governed by Applicable Privacy Laws (with the exception of Data Subjects managing their online privacy preferences (for example, utilizing an unsubscribe button to opt out of communications from Bright Horizons or updating their Cookie settings);

10.1.2. complaints, investigations, or notices of non-compliance with Applicable Privacy Laws from a Data Subject or government authority; and

10.1.3. if permitted under Applicable Law, a request from a public authority to access Client Personal Information.

10.2. As permissible under Applicable Laws, Bright Horizons shall promptly provide all reasonable assistance requested by Client under clause 10.

11. Public Authority Requests.

11.1. Bright Horizons shall not disclose or provide access to Client Personal Information to any public authorities related to international terrorism, counterespionage, surveillance, or foreign intelligence investigation unless required by Applicable Laws. Bright Horizons commits to reviewing the legality of the public authority's request and to challenge such request where lawful and appropriate.

11.2. Where EU/UK Applicable Privacy Laws govern Client Personal Information and a request under clause 11.1 is incompatible with Article 46 of the General Data Protection Regulation, Bright Horizons shall inform the public authority of the same.

12. Sub-processors.

12.1. Subject to clauses 12.2 to 12.5, Client acknowledges and agrees that Bright Horizons may retain as necessary Bright Horizons' Affiliates located in the United Kingdom, United States and India as Sub-processors and Bright Horizons and/or Bright Horizons' Affiliates may engage third-party Sub-processors.

12.2. Bright Horizons shall ensure that any Sub-processor:

12.2.1. has agreed contractual terms with Bright Horizons which are materially equivalent and offer equivalent protection to such Client Personal Information as afforded under the DP Terms and Applicable Privacy Laws; and

12.2.2. takes all information security and privacy measures required under Applicable Privacy Laws and the DP Terms.

12.3. If any Sub-processor fails to comply with Applicable Privacy Laws and/or applicable obligations under the DP Terms, Bright Horizons shall remain liable to Client for the performance of that Sub-processor's obligations.

12.4. Bright Horizons' current list of Sub-processors is at https://www.brighthorizons.com/privacy-security/sub-processors.

12.5. Unless a Sub-processor is an Emergency Replacement, Bright Horizons shall notify Client in advance of changes as required under Applicable Privacy Laws, providing sufficient information about the Sub-processor to enable Client to determine whether it objects to the change. For Emergency Replacements, Bright Horizons shall notify Client as soon as practicable. If Client objects within fifteen (15) business days of receipt of the notice, the parties shall work together in good faith to resolve the objection. If the parties cannot reach an agreement, for reasonable objections based on information security/privacy grounds that are appropriate to the Processing risks, Client may require Bright Horizons to cease the affected Processing.

13. Service Provider Certification: Bright Horizons certifies that it understands and shall comply with its obligations under Section C of the DP Terms and shall notify Client if it makes the determination that it can no longer meet its obligations under Applicable Privacy Laws for Client Personal Information. Where Bright Horizons has provided such notification to Client, Client may take reasonable and appropriate steps to stop and remediate Bright Horizons' unauthorized use of Client Personal Information

14. Third Country Transfers. As required under Applicable Privacy Laws, Bright Horizons makes available the transfer mechanisms identified in Annex B as applicable. In the event of any conflict

or inconsistency between the DP Terms or Annex B and the applicable transfer mechanism, the transfer mechanism shall prevail to the extent necessary to resolve such conflict. If under Applicable Privacy Laws, a transfer to Bright Horizons, a Bright Horizons Affiliate or a Sub-processor constitutes an onward transfer of Client Personal Information, Bright Horizons represents and warrants that there are enforceable and written contractual agreements in place which comply with the requirements under the applicable transfer mechanism.

Section D – Bright Horizons Personal Information

15. Bright Horizons Personal Information. In respect of Bright Horizons Personal Information received by (or on behalf of) Client, Client agrees:

15.1. not to Sell or Share such Bright Horizons Personal Information;

15.2. not to attempt to or re-identify any previously aggregated, deidentified, or anonymized Bright Horizons Personal Information except as specifically agreed in writing between the parties; and

15.3. except as required by an Applicable Law to which Client is subject (and notified in writing to Bright Horizons), not to Process such Bright Horizons Personal Information other than as reasonably necessary and proportionate for the purposes of fulfilling its obligations under the Agreement; receiving the benefits under the Agreement; or managing or administering the Services.

Section E - Information Security

16. Security Measures. Bright Horizons shall implement appropriate administrative, technical, physical, organizational and operational safeguards and other security measures designed to (i) ensure a level of security appropriate to the risk presented by the Processing of Personal Information; (ii) protect against any anticipated threats or hazards to the security, availability, confidentiality and integrity of Personal Information; and (iii) protect against Security Incidents ("Security Measures").

16.1. The Security Measures shall comply with all Applicable Privacy Laws and take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing, as well as the risk of varying likelihood and severity for the rights and freedoms of Data Subjects, including as appropriate (i) the pseudonymisation and encryption of Personal Information; (ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services; (iii) the ability to restore the availability and access to Personal Information in a timely manner in the event of a physical or technical incident; and (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing.

16.2. Annex A details the Security Measures in place as at the date of the DP Terms. For the duration of the Processing, Bright Horizons shall maintain the Security Measures which are at least as protective as those outlined in Annex A and as required under Applicable Privacy Laws.

16.3. Bright Horizons shall supervise and/or train as appropriate any parties it authorises to Process Personal Information, to the extent necessary to maintain appropriate privacy, confidentiality, and security of Personal Information.

17. PCI Compliance. To the extent Bright Horizons Processes payment account information or cardholder data, it shall perform the services in compliance with the payment card industry data

security standard ("PCIDSS") and any subsequent versions, updates or modifications thereto, and hereby acknowledges its responsibility for the security of any cardholder data (as such term is defined in the PCIDSS) that it Processes in connection with the Services.

18. Disaster Recovery Plan. Bright Horizons warrants and represents that it has and shall maintain an appropriate disaster recovery, business continuity and contingency plan and related policies and procedures (collectively, the "DR Plan"). The DR Plan shall provide for continued operation in the event of a catastrophic event affecting Bright Horizons' business operations and shall be in accordance with internationally accepted business continuity, contingency and disaster recovery planning standards, procedures, and practices. Upon Client's written request, Bright Horizons shall furnish a written summary of its DR Plan.

19. Information Security and Privacy Audit. Subject to clauses 19.1 – 19.4, Bright Horizons shall make available to Client all information reasonably necessary to demonstrate compliance with its obligations under the DP Terms and allow for and contribute to audits as reasonably necessary. Bright Horizons shall inform Client if in its opinion, an instruction infringes on Applicable Privacy Laws.

19.1. Subject to clause 19.2, upon Client's written request (but not more than annually unless there is a Security Incident), Bright Horizons shall (and as relevant require its Sub-processors to) participate in Client's information security and privacy audit.

19.2. Bright Horizons shall make available to Client the current Third Party Certifications as evidence of its compliance with these DP Terms. Only if Client demonstrates that the information available in Annex A and the Third Party Certifications are not sufficient to evidence compliance with the DP Terms as required by Applicable Privacy Laws, Bright Horizons shall:

19.2.1. participate in Client's information security and privacy questionnaire, providing accurate and timely responses with supporting evidence as reasonably requested; and

19.2.2. facilitate and allow Client to perform an onsite or remote interactive assessment at its relevant premise(s) provided that such assessment shall: (a) be no longer than one (1) eight hour business day; (b) be within normal business hours; (c) not unreasonably disrupt Bright Horizons' business or operations; (d) not infringe on Bright Horizons' obligations under Applicable Privacy Laws or contract; (e) have the scope agreed by both parties in advance (with agreement not to be unreasonably withheld or delayed by either party) and (f) exclude on-site / remote interactive inspections of multi-tenant environments (such as data centers or other shared services used by Bright Horizons).

19.3. In relation to clause 19.2.2(f) above, Bright Horizons will provide, upon Client's written request, documentation which Bright Horizons used to evaluate the data protection and security measures of the provider of such environment.

19.4. Client shall promptly notify Bright Horizons of any non-compliance identified under clause 19.2.

19.5. Client agrees (and shall ensure its designees agree) not to perform any vulnerability and penetration testing, phishing or social engineering attacks on the hardware, software, facilities, and personnel of Bright Horizons or any of its Affiliates or Processors or Sub-

processors. Any such activity is unauthorized and if appropriate under Applicable Laws, Bright Horizons may report such activity to the relevant government authorities.

20. Security Incident.

20.1. In the event of any Bright Horizons' Security Incident involving Personal Information, Bright Horizons shall:

20.1.1. promptly take all reasonably necessary and appropriate investigative and corrective actions to remedy the underlying causes and mitigate the impact of the Security Incident; and

20.1.2. where the Security Incident requires notification to Data Subjects and/or a government authority under Applicable Privacy Laws, notify Client without undue delay.

20.2. In addition to clause 20.1, in the event of any Bright Horizons' Security Incident involving Client Personal Information, Bright Horizons shall:

20.2.1. notify Client within two (2) business days or such shorter period as reasonably required for Client to comply with Applicable Privacy Laws;

20.2.2. provide timely updates to Client on its investigation;

20.2.3. cooperate as reasonably requested with Client's investigation into the Security Incident; and

20.2.4. if permitted by Applicable Law, make no notice of the Security Incident to any other third party without the written permission and direction of Client.

20.3. Any notices to Client required under clauses 20.1 and 20.2 shall summarize in reasonable detail the nature and impact of the Security Incident.

20.4. If required by Applicable Privacy Laws, Bright Horizons shall notify the Security Incident to the competent government authority and/or affected Data Subject(s). Bright Horizons shall be responsible for the costs and expenses associated with its obligations described in this clause 20.4, unless and to the extent the Security Incident is caused by the acts or omissions of Client.

Section E – Bright Horizons' Notifications

21. Notifications: In order to receive any notifications from Bright Horizons under the DP Terms, Client must subscribe at https://go.brighthorizons.com/information-security-and-privacy-notifications and keep such subscription updated. Notwithstanding any other term of the Agreement, notifications under the DP Terms will be by email to the currently subscribed email addresses provided by Client using this form.

Section E - Definitions

22. Unless otherwise provided expressly in this clause or the DP Terms (including the Annexes), terms used in the DP Terms shall bear the meanings ascribed to them in the Agreement:

22.1. **Affiliate:** means any entity that directly or indirectly controls, is controlled by, or is under common control with another entity;

22.2. **Applicable Privacy Laws:** means Applicable Laws protecting the fundamental rights and freedoms of Data Subjects' privacy;

22.3. **Applicable Laws:** means the legislation, national implementing laws, regulations and secondary legislation (including, where applicable, statutes, decisions, guidelines, guidance notes, codes of practice, codes of conduct and data protection certification mechanisms issued by courts and other applicable authorities), as amended or replaced from time to time and as applicable to a party to the Agreement;

22.4. **Authorised Affiliates:** means any of Client's Affiliate(s) which is permitted to use the Services pursuant to the Agreement but is not defined as "Client" under the DP Terms;

22.5. **Bright Horizons:** means the Bright Horizons Affiliate which is party to the Agreement;

22.6. **Bright Horizons Personal Information:** means Personal Information which Bright Horizons acts as the Controller or Business under the Agreement;

22.7. **Business** means as defined under Applicable Privacy Laws;

22.8. **Business Contact Information:** means the names, job roles, mailing addresses, email addresses, phone numbers and other contact information regarding the other party's employees, directors, vendors, agents and customers.

22.9. **Client:** means the entity which entered into the Agreement and, for the purposes of the DP Terms only, and except where indicated otherwise, the term "Client" shall include Client and Authorised Affiliates;

22.10. **Client Personal Information:** means Personal Information which Bright Horizons acts as Processor or Service Provider on behalf of Client as identified in Annex C;

22.11. **Controller:** means as defined under Applicable Privacy Laws or any entity which (i) determines the purposes and means of the Processing of the Personal Information; or (ii) is a Business.

22.12. **Data Subject:** means a natural person whose Personal Information is being Processed under the Agreement;

22.13. **Emergency Replacement**: means when Bright Horizons requires a sudden replacement of a Sub-processor to continue providing the Services;

22.14. **Personal Information**: means any information (i) that is received, stored or otherwise Processed under the Agreement or in connection with the Services; and (ii) relates to an identified or identifiable natural person an identifiable natural person is one who can be identified, directly or indirectly or as the jurisdiction or circumstances permit, any other personally identifiable information;

22.15. **Processing, Process and Processed:** means any operation or set of operations which is performed on Personal Information or on sets of Personal Information, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction, or as otherwise defined under Applicable Privacy Laws;

22.16. **Processor:** means as defined under Applicable Privacy Laws or any entity which (i) Processes Personal Information on behalf of another entity; and / or (ii) is a Service Provider;

22.17. **Security Incident:** means a breach of security leading to any accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Information;

22.18. **Security Measures:** means as defined in clauses 18;

22.19. **Sell:** means as defined under Applicable Privacy Laws;

22.20. **Service Provider**: means as defined under Applicable Privacy Laws;

22.21. **Share:** means as defined under Applicable Privacy Laws;

22.22. **Sub-processor:** means another Processor engaged by Bright Horizons to Process Client Personal Information on its behalf; and

22.23. Third Country Transfer: means the transfer of Client Personal Information that originates in the European Economic Area and/or the United Kingdom to outside the applicable jurisdiction.

22.24. Third Party Certifications: means third-party certifications and audits set forth in Annex A.

ANNEX A: BRIGHT HORIZONS INFORMATION SECURITY MEASURES

Overview and Security Program Objectives

Bright Horizons' Information Security program is a combination of policy, security architecture and descriptions of current IT security services and control practices. The overall program describes administrative, operational, and technical security safeguards that must be implemented wherever we process or store sensitive or private information.

The Bright Horizons Information Security Office's mission is to provide Bright Horizons with the highest quality service and sound technical direction that:

- **Provide security to protect our organization, clients and families**
- **Support growth**
- **Create efficiencies**

Our information security program, based on the ISO 27001 framework is designed to effectively safeguard that information.

The Bright Horizons Information Security Program receives full support from company management and the Board.

Information Security is an integral part of our service delivery

We are responsible for the safekeeping of something that our clients and families consider extremely important: their children and personal information about the families.

Bright Horizons is the only publicly traded child-care company in the United States (NYSE: BFAM) and is compliant to all provisions of the Sarbanes-Oxley act. We fully comply with the EU General Data Protection Regulation (GDPR) regarding scoped data that is transferred to the United States.

Our commitment to information security enables us to have dedicated information security and privacy teams with the policies, people and processes in place that stand up to the high standard set by our clients in the Fortune 500.

Our Security program is ISO 27001 and SOC 2 Type 2 certified. Our Privacy program is ISO 27701 certified.

We believe our information security posture far exceeds anything that our competitors are capable of achieving.

Our information security program is described in the following pages. If you have any questions or need additional details, please feel free to contact me.

Sincerely,
Javed Ikbal, CISSP, CISM, CISA
CISO

Security Domains of the Bright Horizons Information Security Program

Policy

The foundation of our Information Security Program is built upon the **Acceptable Use Policy** and the **Managing and Storing Protected Information Policy** documents. These policies are additionally supported by a full range of other relevant policies, standards and guidelines.

The policies and supporting documents provide direction and support for information security in accordance with business requirements and relevant laws and regulations.

Organization of Information Security

A structured management framework provides oversight over the information security function at Bright Horizons. The CEO of Bright Horizons is the executive sponsor of the Information Security Program. The Information Security function also submits an annual report to the Audit Committee of the Board.

Information Security is led by the CISO, an experienced professional with decades of experience in the field. The CISO also co-chairs the Privacy and Security Steering committee, a cross-functional team with representatives from Privacy, Legal, Internal Audit and Information Technology.

Asset Management

The Information Security Program document describes individual responsibilities for managing and inventorying our physical and logical assets.

A matrix is available to assist system and data owners to appropriately classify the sensitivity of their information.

Bright Horizons does not collect social security numbers for any of its Client-facing services. Bright Horizons outsources payment collection to established financial institutions, and does not store or process credit card numbers or bank account information for its Clients' employees.

Human resources security

Prior to commencing employment, employees and contractors undergo background checks. Users are also educated about the acceptable uses of technology. All employees and contractors are required to sign a confidentiality agreement.

During employment, employees, contractors and third party users with access to Bright Horizons Technology and Information are made aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support the information security Program in the course of their normal work.

Policies and other requirements are provided to each employee during orientation and are available on the company's Intranet site. Any employee who fails to comply with any of these policies is subject to termination. Each employee needs to agree with the updated policies.

Physical and environmental security

The Bright Horizons Information Security Program addresses unauthorized physical access, damage and interference to the organization's premises and information, as well as the loss, damage, theft or compromise of assets and interruption to the organization's activities.

All our corporate offices have video monitoring of all perimeter access doors and alarms. Visitors must be approved by an employee, and must be escorted.

To ensure uptime and availability, all of our clients-facing applications are hosted in data holding facilities that are tier-3 co-location facilities and are SOC 2 certified. Datacenter SOC 2 reports are available upon request.

The co-location data centers have 24x7 guard patrols, alarms, live video monitoring and multiple levels of physical access control. The data centers are equipped with N+1 generators, N+1 UPS systems, smoke and fire detection and suppression systems. Power is supplied from two separate substations.

We back up data across the network between our primary and backup data centers. This eliminates the risk of losing backup tapes during transportation or the risk of using 3rd-party offsite storage.

Communications and operations management

In order ensure the correct and secure operation of information processing facilities, Bright Horizons' Information Security Program includes the following communications and operations management section:

Vendor security and third party service delivery management

For both current and prospective vendors, we first evaluate whether they will hold, transmit, or have exposure to personally identifiable information or financial information for either our clients or employees. If they do, they are required to complete a Bright Horizons supplier security questionnaire (SSQ), which was developed from a variety of SSQs required by our clients. The questions ensure that our vendors meet the industry standards and best practices that we expect. Once submitted, the information risk team evaluates the organizational risks and creates risk remediation plans. If risks are elevated, we conduct physical site reviews of the data processing and data holding locations. Once all the provisions are satisfied, our information security team will approve the vendor for business with
Bright Horizons. Depending on the risk-level, the process may be repeated annually or every three years.

System planning and acceptance

Our workstations are built from pre-approved images. Servers are built against a security checklist and a vulnerability scan is conducted before they are installed. We have a change management and approval process in place to review and approve any changes in the production environment.

Protection against malicious and mobile code

All our computers have anti-virus and anti-malware products installed. Any mobile devices that can access confidential company information are managed through a mobile device management program and are required to be password-locked and encrypted.

Back-up

All our production servers and databases are backed up to maintain the availability and integrity of operations

Network security management

We have perimeter and internal network security devices such as firewalls and intrusion prevention systems in place to detect and block attacks.

Media handling

We do not use tapes for backup, and as a result do not require any off-site transportation. We prohibit the storage of confidential information on unencrypted portable media. All our laptops have full-disk encryption. Only authorized mobile phones encrypted with our MDM solution may access company information.

Exchange of information

We use TLS for email communication with parties that support it. Confidential information may also be sent over S/MIME encrypted email.

All web communication containing personal or confidential data is SSL-encrypted. If we regularly exchange files containing personal information with a Client, we use SFTP, sometimes after PGPencrypting the file.

Monitoring

We log significant events on our information processing systems and monitor the logs for indications of confidentiality, availability and integrity breach of the data.

Access Control

Access control is set for least privilege based on employees' roles. Access to confidential information requires manager's approval. For employees in IT admin functions, separate administrator user accounts are created in addition to their employee user accounts. When employees, contractors and third party users have a role change or exit Bright Horizons, specific processes exist to modify or terminate access expeditiously.

User access entitlements to Client information and critical systems are reviewed quarterly.

Information systems acquisition, development and maintenance

The Bright Horizons Information Security Office sets the security requirements for our applications according to industry best practices.

For most of our applications, we encrypt the data at rest. Passwords are always stored in a salted hash form in our applications.

Development staff does not have access to production systems unless specifically authorized for troubleshooting. We have an established process for scrubbing the data to remove any personally identifiable information before moving the data from Production to non-production environments.

Before rolling out a newly developed product, we conduct a thorough application security review to ensure there are no vulnerabilities. After that, we conduct security reviews after any major changes and also annually.

We monitor various information sources for newly announced vulnerabilities, and patch and/or establish compensating controls. We scan our network and infrastructure monthly to identify vulnerable systems.

Information security incident management

Bright Horizons maintains a comprehensive incident management program that is tested and updated regularly. This allows us to ensure a consistent and effective approach is applied to the management of information security incidents, and to meet our obligations to notify Clients and our families.

Disaster Recovery and Business Continuity:

The Information Security Office works in conjunction with IT, business operations, risk management and
HR to ensure proper business continuity during a disaster event. Critical systems availability at Bright Horizons is protected by several redundant and resilient components, including local High Availability setups, Hot-Warm configuration between our production and backup data centers, and periodic snapshots of the database and nightly backups.

Our primary and backup data centers are located 1,800 miles apart, and we replicate data between our facilities for disaster recovery purposes.

We contract with a national disaster recovery company to provide us a trailer-mounted office and recovery facility if needed to recover essential business functions.

Bright Horizons has identified recovery time objectives and recovery point objectives for our corporate systems and our client-facing systems. Every critical system server has a 24x7 vendor support contract to ensure availability of replacement parts within four (4) hours to minimize system downtime.

We test our response to a disaster annually.

Compliance

Our information security program is designed to comply with all relevant laws, statutory, regulatory or contractual obligations and of any security requirements.

The program ensures compliance of our information systems with organizational security policies and standards, and strives to maximize the effectiveness of and to minimize interference to/from the information systems audit process.

We are audited by Bright Horizons' internal and external auditors, and undergo assessments by many of our Clients including Clients from the financial and defense sectors. All Client audits are conducted according to the audit clause as specified in the contract with the Client.

Appendix: Data Elements

The following data elements are collected for various Bright Horizons services:

	Back-up Care	Center / Nursery	EdAssist	College Coach	Special Needs	Parental Leave Toolkit	Work + Family Space (incl. coaching)	EFS
Name	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Phone number	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Email address	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Employee ID #	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Educational Records (Transcripts)	No	Yes	Yes	Yes	Yes	No	No	No
Name of child	Yes	Yes	No	Yes	Yes	No	Voluntary	No
DOB of child	Yes	Yes	No	Yes	Yes	Yes	No	No
Gender of child	Yes	Yes	No	Yes	Yes	No	Voluntary	No
Emergency contact	Yes	Yes	No	No	No	No	No	No
Dietary restrictions	Yes	Yes	No	No	No	No	No	No
Payment Information	Yes	Yes	Yes	Yes	No	No	No	No
Government Identifiers	No	Yes	No	No	Voluntary	No	No	No
Sexual Orientation	No	Voluntary	No	Voluntary	No	No	Voluntary	No
Health Data	Yes	Yes	No	Voluntary	Yes	Yes	Voluntary	No
Religious beliefs	Voluntary	Voluntary	No	Voluntary	No	No	Voluntary	No
Race/ethnic origin	Voluntary	Voluntary	No	Voluntary	No	No	Voluntary	No
Care records	No	Yes	No	No	No	No	No	No
Trade union membership	No	No	Voluntary	No	No	No	No	No

Key:

Yes	Required in order to provide the Service
No	Not collected
Voluntary	Provided at the discretion of the individual / their employer
Sensitive PI	Sensitive Personal Information

ANNEX B1: UK CONTROLLER TO PROCESSOR TRANSFER MECHANISMS FOR UK CLIENT PERSONAL INFORMATION

1. This Annex B1 applies where Client is exporting Client Personal Information from the United Kingdom (UK) to another country that does not benefit from an adequacy decision pursuant to Applicable Privacy Laws. Bright Horizons makes available the following transfer mechanisms:

1.1. the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the Commissioner under S119A(1) Data Protection Act 2018 and in force as of 21 March 2022 ("**UK Addendum**"); or

1.2. the Standard Data Protection Clauses issued by the Commissioner under S119A(1) Data Protection Act 2018 International Data Transfer Agreement in force 21 March 2022 ("**UK IDTA**").

2. Where any Third Country Transfer would otherwise be in breach of Applicable Privacy Laws, the UK IDTA or the UK Addendum executed by Bright Horizons Family Solutions LLC are available here: https://www.brighthorizons.com/privacy-security and is incorporated herein.

3. Client's signature on the Agreement shall be deemed the execution and acceptance of the UK IDTA or the UK Addendum under clause 2 above by Client (and to the extent required under Applicable Privacy Laws, in the name of and on behalf of its Authorised Affiliates).

4. For the purpose of the UK Addendum:

4.1. For Table 1, Client or its Authorised Affiliate shall be the "Exporter" and Client's contact details as registered by the Client with Bright Horizons as the Privacy contact at: https://go.brighthorizons.com/information-security-and-privacy-notifications

4.2. Table 2 of the UK Addendum shall be deemed to read as follows: The version of the Approved EU SCCs which this Addendum is appended to shall be the EU SCCs specified in Annex B2 to the DP Terms.

5. For the purpose of the UK IDTA:

5.1. Client or its Authorised Affiliate shall be the "Exporter";

5.2. Client's contact details for the purposes of Table 1 of the UK IDTA shall be as registered by the Client with Bright Horizons as the Privacy contact at: https://go.brighthorizons.com/information-security-and-privacy-notifications

5.3. The Categories of Personal Data (including any Special Category Personal Data) which is Transferred Data; Relevant Data Subjects; and Purposes of Processing in Table 3 of the UK IDTA shall be as specified in the applicable fields of the Annex C to the DP Terms;

5.4. The Security Requirements under Table 4 of the UK IDTA shall be as outlined at Clauses 16 to 18 and Annex A to the DP Terms;

5.5. Client acknowledges and expressly agrees that:

5.5.1. clause 8 of the DP Terms (and instructions in accordance therewith) shall govern the implementation of Section 12.1.1 of the UK IDTA;

5.5.2. Bright Horizons and Bright Horizons' Affiliates shall engage Sub-processors in accordance with clause 12 of the DP Terms;

5.5.3. the deletion of Client Personal Information required under Section 31.2.2 shall be completed in accordance with clause 9 of the DP Terms.

ANNEX B2: EEA CONTROLLER TO PROCESSOR TRANSFER MECHANISMS FOR EU CLIENT PERSONAL INFORMATION

1. This Annex B2 applies only to where Client is exporting Client Personal Information from the European Economic Area (EEA) to another country that does not benefit from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 ("GDPR"). Bright Horizons makes available the following transfer mechanism: standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council as approved by the European Commission under Decision (EU) 2021/914 of 4 June 2021 ("**EU SCCs**").

2. Where any Third Country Transfer would otherwise be in breach of the GDPR, the EU SCCs executed by Bright Horizons Family Solutions LLC are available here: https://www.brighthorizons.com/privacy-security and are incorporated herein.

3. Client's signature on the Agreement shall be deemed the execution and acceptance of the EU SCCs under clause 2 above by Client (and to the extent required under Applicable Privacy Laws, in the name of and on behalf of its Authorised Affiliates).

4. For the purpose of the EU SCCs:

4.1. Client or its Authorised Affiliate shall be the "data exporter" for the cover page and Annex 1.A of the EU SCCs;

4.2. Client's contact details for the purposes of Annex 1.A of the EU SCCs shall be as registered by the Client with Bright Horizons as the Privacy contact at: https://go.brighthorizons.com/information-security-and-privacy-notifications

4.3. the applicable Annex(es) C of the DP Terms shall be Annex 1.B of the EU SCCs;

4.4. Annex A of the DP Terms shall be Annex II of the EU SCCs;

4.5. Client acknowledges and agrees:

4.5.1. Processing instructions: as applicable, clause 8 of the DP Terms (and instructions in accordance therewith) shall govern the implementation of clauses 8.1 and 8.2 of the EU SCCs;

4.5.2. Accuracy of Client Personal Information: as applicable, clause 10 of the DP Terms shall govern the implementation of clause 8.4 of the EU SCCs;

4.5.3. Duration of Processing and retention of Client Personal Information: as applicable, clause 9 of the DP Terms shall govern the implementation of clause 8.5 of the EU SCCs;

4.5.4. Security of Client Personal Information: as applicable, clauses 16 and Annex A of the DP Terms shall govern the implementation of clause 8.6 and Annex II of the EU SCCs;

4.5.5. Onward Transfers: as applicable, clauses 12 and 14 of the DP Terms shall govern the implementation of clause 8.8 of the EU SCCs;

4.5.6. Documentation and compliance: as applicable, clauses 4 and 19 of the DP Terms shall govern the implementation of clause 8.9 of the EU SCCs;

4.5.7. Sub-processors: as applicable, clause 12 of the DP Terms shall govern the implementation of clause 9 of the EU SCCs;

4.5.8. Data Subject Rights: as applicable, clause 10 of the DP Terms shall govern the implementation of clause 10 of the EU SCCs; and

4.5.9. assessments required under clause 14 of the EU SCCs are available upon written request.

ANNEX C1: ELIGIBILITY FILE (IF PROVIDED BY / ON BEHALF OF CLIENT)

Subject matter of Processing:	Eligibility and registration information of Eligible Employees within any Eligibility File sent by Client.
Nature of Processing:	Receipt/use/storage of the Eligibility File as is necessary to comply with the Agreement.
Purpose(s) of Processing:	• To confirm person registering for the Services is the Eligible Employee. • To ensure Eligible Employees are aware of the benefits they are entitled to including sending communications to Eligible Employees such as but not limited to emails, texts, and newsletters. • To create reporting and analytics information that inform Bright Horizons and Client of registration for and use of the Services, as well as for quality improvement of Services (including as necessary anonymization of such Personal Information for these purposes). • Back up, analysis, auditing and accounting activities as necessary to deliver, administer, maintain or improve the Services. • Any other purpose outlined in the Agreement.
Duration of Processing:	For the term of the Agreement and one (1) year thereafter retained in an identifiable format.
Types/Categories of Personal Information (including any sensitive information if applicable):	Employee Name, Work Email address, Employee ID and / or other identifiers as provided by Client and as necessary to confirm eligibility as instructed by Client; demographic information to support reporting analysis which may include special category/sensitive personal information if provided by Client within the Eligibility File.
Categories of Data Subjects:	Employees and other authorized individuals of Client.
Frequency of Transfer:	Continuous basis.
Sub-processors	Bright Horizons' current list of Sub-processors is at: https://www.brighthorizons.com/privacy-security/sub-processors

ANNEX C2: PARENTAL LEAVE TOOLKIT

Subject matter of Processing:	Line manager use of applications to manage Eligible Employees (Application Interaction Data as defined below).
Nature of Processing:	Collection and storage of, and access to and sharing of, the Application Interaction Data (as defined below) as is necessary to provide the Services and comply with the Agreement.
Purpose(s) of Processing:	• To provide the PLTM Services to Client. • To create reporting and analytics information that inform Bright Horizons and Client of registration for and use of the Services, as well as for quality improvement of Services (including as necessary anonymization of such Personal Information for these purposes). • Back up, analysis, auditing and accounting activities as necessary to deliver, administer, maintain or improve the Services.
Duration of Processing:	For the term of the Agreement and up to three (3) years thereafter retained in an identifiable format.
Types/Categories of Personal Information (including any sensitive data if applicable):	Credential and interaction information for line management use of applications to manage Eligible Employees including manager's name, work email address, data in respect of access / use of the application, data uploaded to the manager version of the app in relation to the Eligible Employee by the manager to manage leave plans, such as leave date, due date which is special category/sensitive personal information, return date etc ("Application Interaction Data").
Categories of Data Subject:	Employees and other authorized individuals of Client.
Frequency of Transfer:	On continuous basis.
Sub-processors	Bright Horizons' current list of Sub-processors is at: https://www.brighthorizons.com/privacy-security/sub-processors

ANNEX C3: EDASSIST SERVICES

Subject matter of Processing:	Provision of EdAssist Services to Client's Eligible Employees.
Nature of Processing:	Collection, Processing and storage of such Personal Information directly from the Eligible Employee as is necessary to provide the Services and comply with the Agreement.
Purpose(s) of Processing:	• To provide the Services. • To create reporting and analytics information that inform Bright Horizons and Client of registration for and use of the Services, as well as for quality improvement of Services (including as necessary anonymization of such Personal Information for these purposes). • Back up, analysis, auditing and accounting activities as necessary to deliver, administer, maintain or improve the Services.
Duration of Processing:	For the term of the Agreement and seven (7) years thereafter retained in an identifiable format.
Types/Categories of Personal Information (including sensitive data if applicable):	Name Phone number Email address Employee ID # Educational Records (Transcripts) Payment Information Government Identifiers
Categories of Data Subjects:	Employees and other authorized individuals of Client.
Frequency of Transfers:	On continuous basis.
Sub-processors:	Bright Horizons' current list of Sub-processors is at:https://www.brighthorizons.com/privacy-security/sub-processors

<u>If you wish to execute the DP Terms as a stand-alone Data Processing Agreement ("DPA")</u>:

Please follow the instructions for "*How do clients incorporate the DP Terms into their existing client agreement with Bright Horizons?*" which are detailed here:

https://www.brighthorizons.com/privacy-security/faqs

The parties hereby execute this DPA as an addendum to the executed agreement between Bright Horizons and Client for the Services ("Agreement").

The effective date of the DPA shall be the date of execution by Client in accordance herewith.

All terms and conditions of the Agreement shall remain in full force and effect subject only to any variations effected by the DPA.

BRIGHT HORIZONS	**CLIENT**
Signature: DocuSigned by: Ann Cartwright B8B6F965DDF443F...	Signature:
By: Ann Cartwright	By:
Title: Global Privacy Officer	Title:
Date: November 28, 2022	Date: