- **privacy-security** faqs

BRIGHT HORIZONS DATA PROTECTION TERMS – FREQUENTLY ASKED QUESTIONS

Bright Horizons Data Processing Terms – Frequently Asked Questions

Does Bright Horizons have Data Protection Terms (DP Terms)?

Yes, click here for Bright Horizons' Data Protection Terms. It sets out the legal framework under which Bright Horizons processes personal information. The DP Terms cover all Bright Horizons' services and are incorporated into our current client agreement forms. Clients who do not have these DP Terms in place are able to sign the DP Terms as a standalone document.

What laws do the DP Terms cover?

The DP Terms cover all applicable privacy laws for our services. The DP Terms are intended to assist clients with their compliance with applicable privacy laws.

Why can clients not use their own Data Protection Agreement when contracting with Bright Horizons?

The Bright Horizons' DP Terms cover the specific processes and procedures for our services and privacy and information security framework. In order to comply with applicable privacy laws, the DP Terms align to Bright Horizons' services, processing activities, and information technology infrastructure / systems. For example, the DP Terms identify and incorporate the transfer mechanisms that Bright Horizons offers to its clients such as the Standard Contractual Clauses and International Transfer Data Agreement. The DP Terms also are drafted to seamlessly integrate with the client agreement and other relevant Bright Horizons' documentation.

Are comprehensive privacy laws applicable to the Services?

Yes. Some comprehensive privacy laws such as the GDPR and CPRA apply to both Bright Horizons and our clients because these laws cover individuals acting in their capacity as employees, as well as in their capacity as consumers.

However, other comprehensive privacy laws (such as in Virginia, Colorado, Utah and Connecticut) only apply to Bright Horizons for certain circumstances because these laws cover individuals acting in their capacity as consumers only. Employees are explicitly excluded from the scope of these laws. To clarify further, where Bright Horizons is acting as the controller for the services it is delivering to the employees of clients (such as Back-up Care, Enhanced Family Services and College Coach), these laws apply to Bright Horizons but not the client. Where Bright Horizons is acting as the processor for the services it is delivering to the employees of the client (such as EdAssist), these laws do not apply to either Bright Horizons or the client.

Which party is the "controller" / "business" or the "processor" / "service provider"?

Comprehensive privacy laws generally distinguish between parties that:

- determine the means and purposes of processing the personal information and refer to these types of parties as "controllers" or "businesses".
- process personal information on behalf of another party and refer to these types of parties as "processors" or "service providers".

Depending upon the service, Bright Horizons acts in the capacity of the controller / business or processor / service provider. Please see the tables below.

Services	Controller / Business or Processor / Service Provider	Applicable comprehensive privacy laws
On-Site Child Care, Back-up Care, Elder Care, College Coach, Special Needs, Additional Family Support, Parental Leave Tool Kit, Work + Family Space, and Coaching Services	Bright Horizons acts as the **controller / business** for all personal information it processes to provide these services (except for the Eligibility File, if applicable – please see below). Bright Horizons determines the purpose and how it processes the personal information.	Comprehensive privacy laws will apply to Bright Horizons as we have a direct relationship with the employee as a consumer of the services. Bright Horizons is acting as the controller / business and the employee is a consumer / data subject as defined under those laws.
EdAssist Services	Bright Horizons acts as the **processor / service provider** for all personal information it processes to provide these services (except for any confidential coaching services for Eligible Employees). The client determines the purpose and how it processes the personal information.	Comprehensive privacy laws which apply to employees (such as the GDPR and the CPRA) will apply to the processing of personal information by Bright Horizons on behalf of the client in order to deliver these services. Comprehensive privacy laws which do not apply individuals acting in their capacity as employees (such as the laws for Virginia, Colorado, Utah and Connecticut) will not apply to the processing of personal information by Bright Horizons on behalf of the client, because the client is acting as the individual's employer in this circumstance, and the individual is acting in the employment context.

Depending upon the processing activities, Bright Horizons acts in the capacity of the controller / business or processor / service provider. Please see the tables below.

Processing Activities	Controller or Processor	Applicable comprehensive privacy laws
Eligibility Files	When a client provides Bright Horizons with an Eligibility File, it does so in the capacity as	Comprehensive privacy laws which apply to employees (such as the GDPR and the CPRA)

	the controller / business. Bright Horizons acts as a processor/service provider in respect of the personal information in that file and processes it as agreed with the client.	will apply to Bright Horizons' processing of the Eligibility File. Comprehensive privacy laws which do not apply individuals acting in their capacity as employees (such as the laws for Virginia, Colorado, Utah and Connecticut) will not apply to Bright Horizons' processing of the Eligibility File.
Client Reports	Where Bright Horizons is the controller / business for the personal information, any such personal information it shares with the client it is sharing such personal information as a controller / business, to the client acting as a separate and independent controller / business.	Where Bright Horizons is the controller / business for personal information shared within reporting, comprehensive privacy laws which apply to individuals acting in their capacity as employees (such as the GDPR and the CPRA) will apply to both Bright Horizons and the client. Under the GDPR, Bright Horizons and the client are not joint controllers in relation to these client reports because each party is processing the personal information for different purposes and do not have joint control of the personal information. Under the CPRA, when Bright Horizons provides this personal information to the client it does so at the eligible employee's direction (in accordance with Bright Horizons' privacy notice) for the purposes of Bright Horizons delivering the requested services to the consumer and the client administering the benefit. Therefore, this provision of personal information by Bright Horizons to the client does not constitute "sharing" or "selling" of personal information as defined under the CPRA. Comprehensive privacy laws such as for Virginia, Colorado, Utah and Connecticut which do not apply to individuals acting in their capacity as employees do not apply to Bright Horizons sharing of personal information with the client as the personal information is being shared for the purposes of administering the benefit(s).

How do the DP Terms comply with requirements of various applicable privacy laws where Bright Horizons is processing personal information on behalf of its clients?

Comprehensive privacy laws set out specific requirements directly on a third party processing personal information on behalf of another (ie: the processor / service provider). These are in addition to the requirements placed on the party which determines the means and purposes of the processing (controller / business). The table below identifies the clauses in the DP Terms that relate to each of these specific contractual requirements under the relevant comprehensive privacy laws (GDPR and CCPA/CPRA) for all contracts between controllers / businesses and processors / service providers.

Requirement	**GDPR Articles**	**CCPA / CPRA Sections**	**DP Terms Clauses / Annexes**
Contract between controller/business and processor/service provider shall include: **instructions for processing data**, the nature and purpose of processing, the type of data subject to processing, the duration of processing.	Article 28(3)	1798.140 (ag)(1)(B)	Annex C
Processor/service provider only to **process the personal information on instructions** from the controller/business or as required by law.	Article 28(3)(a)	1798.140 (ag)(1)(B) & (C)	Clauses 3, 6 and Annex C
Processor/service provider not to attempt to **re-identify** any de-identified (anonymous) data.	Article 28(3)(a)	1798.140 (m)©	Clause 6.2.1
Processor/service provider not to **sell** the personal information or to **share** the personal information with third parties for the purposes of cross-context behavioral advertising.	Article 28(3)(a)	1798.140 (ag)(1)(A)	Clause 6.2.2
Processor/service provider not to **combine** the personal information.	-	1798.140 (ag)(1)(D)	Clause 6.2.3
Processor/service provider only to **transfer the personal information on instructions** from the controller/business or as required by law.	Article 28(3)(a)	-	Clauses 6, 10 12 and Annexes B and C
Processor/service provider to **retain personal information only for the period required** in connection with the provision of services to controller/business.	Article 28(3)(g)	1798.140 (ag)(1)(B)	Clauses 3 and 7
Controller/business shall use only processors/service providers providing sufficient guarantees to implement appropriate **technical and organisational**	Article 28(1)	1798.100. (e) together with 1798.100. (d)	Clauses 3, 14 and Annex A

measures to protect the personal information.			
Processor/service provider to ensure applicable security measures in place and assist the controller/business as necessary in ensuring **compliance with all required security measures**.	Article 28(3)(c)&(f)	1798.100. (e) together with 1798.100. (d)	Clauses 3, 14 and Annex A.
Processor/service provider to **make available to the controller/business all information necessary to demonstrate compliance** with the required obligations including as applicable, contributing to **audits / inspections** and / or providing copies of relevant **reports / certifications**.	Article 28(3)(h)	1798.140 (ag)(1)	Clauses 3, 14, 17 and Annex A.
Processor/service provider to ensure that persons authorised to process the personal information are under **an obligation of confidentiality**.	Article 28(3)(b)	-	Clause 4
Processor/service provider to assist the controller/business in the fulfilment of the latter's obligation to **respond to requests from a data subject**.	Article 28(3)(e)	1798.105(c)(3)	Clauses 3 and 8
Processor/service provider to assist the controller/business in the fulfilment of the latter's obligation to complete required **impact assessments** concerning the risks connected to the processing of the personal information.	Article 28(3)(f)	-	Clauses 3, 14, 17 and Annex A
Processor/service provider to assist the controller/business in the fulfilment of the latter's obligation to make required **notifications in relation to breaches** of security affecting the personal information.	Article 28(3)(f)	-	Clause 18
Processor/service provider to notify controller/business of any other processor/service provider it intends to instruct to process the personal information (**Sub-Processor**), with opportunity for controller/business to object if applicable.	Article 28(2) and (3)(d)	1798.140 (ag)(2)	Clause 10.4
Processor/service provider to ensure appropriate privacy obligations reflecting those set out in the contract between the controller/business and the	Article 28(4) and (3)(d)	1798.100 (d) and	Clause 10.2.1

processor/service provider **are imposed on that other processor**.		1798.140 (ag)(2)	
Processor/service provider to remain **fully liable** to controller/business for Sub-Processor's performance of obligations.	Article 28(4) and (3)(d)	1798,145 (i)(1)	Clause 10.3
Processor/service provider to notify controller/business if former makes a determination that it can **no longer meet its obligations** under the applicable privacy law.	-	1798.100. (d)(4)	Clause 11
Controller/business to have right to take reasonable and **appropriate steps to stop and remediate unauthorized use** of personal information if a notification is received from the processor/service provider that it can no longer meet its obligations under the applicable privacy law.	-	1798.100. (d)(4)	Clause 11

How do clients incorporate the DP Terms into their existing client agreement with Bright Horizons?

The wording in our current client agreement forms incorporates the DP Terms by specific reference and, accordingly, when the client executes the client agreement it is also executing the DP Terms.

For those desiring to sign the DP Terms as a standalone document, the online DP Terms are pre-signed by Bright Horizons. In order to execute the DP Terms, the client may: either click here to sign using DocuSign or download the DP Terms here and then complete, sign and return it to dataprivacy@brighthorizons.com.

Please note that where the DP Terms are incorporated into the client agreement, the client will not need to sign and return the DP Terms to dataprivacy@brighthorizons.com.

What happens if my organization does not agree to the DP Terms?

Bright Horizons reserves the right to not enter into an agreement (or renew an agreement) for services with the client if the client does not agree to the DP Terms. For any updates to the DP Terms, if a client objects to them, Bright Horizons reserves the right to terminate the agreement or the provision of relevant services.

How does Bright Horizons lawfully transfer personal information outside of the EU?

On 13 July 2020, the Court of Justice of the European Union confirmed the validity of the European Commission's standard contractual clauses as a legal mechanism for transferring personal information outside of the European Economic Area (provided that a risk assessment confirms adequate protection is in place) but invalidated the EU-US Privacy Shield framework. This means that companies

may not rely on the EU-US Privacy Shield framework at present. However, Bright Horizons clients may continue to use our services, relying on the European Commission's Standard Contractual Clauses and / or the UK's Standard Data Protection Clauses / International Data Transfer Addendum, along with Bright Horizons' relevant risk assessment for adequate protection. In relation to transfers to the United States of America, Bright Horizons remains certified to the EU-US Privacy Shield Framework, and accordingly obligated to comply with its privacy framework. As of the publication date of these FAQs, an adequacy decision by the European Commission in respect of the Trans-Atlantic Data Privacy Framework ("the Framework") remains pending. As and when the European Commission issues an adequacy decision in respect of the Framework (and, for UK transfers, the applicable UK authorities approve use of such Framework), Bright Horizons shall work towards making such Framework available to its clients as an alternative mechanism to transfer personal information from the UK and / or EEA to the US.

What about onward transfers of personal information?

Where the transfer to Bright Horizons constitutes an onward transfer, meaning the client exported personal information from the European Economic Area or the UK before transferring it to Bright Horizons, Bright Horizons has in place written contractual agreements with its processors which covers the obligations required under the Standard Contractual Clauses to the extent relevant.

What is your process for responding to Public Authority Requests?

Please see our Transparency Report, available here.

Under the DP Terms, how does Bright Horizons notify clients of new sub-processors or notifiable breaches?

If clients register using this form, they will receive notifications on new sub-processors or notifiable breaches as requested. clients may register more than one contact.

How does Bright Horizons validate its information security program?

- Bright Horizons is a public company (NYSE: BFAM) and must comply with the Sarbanes-Oxley Act of 2002 (SOX).Section 404 of SOX mandates that all publicly traded companies establish internal controls and procedures for financial reporting and must document, test and maintain those controls and procedures to ensure their effectiveness. A third-party auditor reviews and provides an opinion as to the validity of the company's assertions in this internal control report.

- COBIT (Control Objectives for Information and Related Technologies) is a best practice framework and toolset created by ISACA to support information technology management and governance. As part of Bright Horizons SOX audit, our internal audit team, and an independent third party, conduct annual COBIT audits, validating Bright Horizons' compliance with our information security programme.

- SOC 2 reporting is an attestation of a company that certain controls are in place to meet as relevant the AICPA's (American Institute of Certified Public Accountants) SOC Trust Services Criteria and includes the opinion of an independent Certified Public Account. This type of report covers the control systems in place to safeguard unauthorized access (both physical

and logical) for data and systems availability for operation and use as committed by the company. A third party auditor conducts a SOC 2 audit on Bright Horizons annually.

- Bright Horizons' Information Security program is ISO 27001 certified: ISO/IEC 27001 is the international standard for information security. It sets out the specification for an information security management system (ISMS). ISO 27001's best-practice approach helps organisations manage their information security by addressing people, processes, and technology. Certification to the ISO 27001 Standard is recognised worldwide to indicate that an ISMS is aligned with information security best practices. Part of the ISO 27000 series of information security standards, ISO 27001 is a framework that helps organisations establish, implement, operate, monitor, review, maintain and continually improve an ISMS. The certificate is available here.

- Bright Horizons' Privacy program is ISO 27701 certified: ISO/IEC 27701 is a privacy extension to the international information security management standard, ISO/IEC 27001. ISO 27701 specifies the requirements for – and provides guidance for establishing, implementing, maintaining and continually improving – a PIMS (privacy information management system). ISO 27701 is based on the requirements, control objectives and controls of ISO 27001, and includes a set of privacy-specific requirements, controls and control objectives. The certificate is available here.

Where does Bright Horizons store its personal information?

- Electronic

Some personal information may remain on electronic storage data systems in the country where we provide the service. However, our primary electronic storage facilities and contact centers are located in the United States.

- Hardcopy

The hardcopy of personal information we collect remains in the country where the individual receive the services or provide the information.

Who are Bright Horizons sub-processors?

Click here for information on Bright Horizons sub-processors.

Download a copy of these FAQs here