

Terms and conditions

1. What this agreement is about;

- i. This agreement describes how the User may use Bright software products.
- ii. In this agreement, "Bright software products" refers to the on-line human resources (HR) and Health and Safety software and the "Services".
- iii. "Services" refers to the provision of the Provider's website and other digital services, associated software, and other services provided by the Provider in accordance with these Terms of Use, together with the characteristics and features as described at www.brighthr.com from time to time. The User understands and agrees that it cannot use a Service unless it is licensed by the Provider to use and has paid the applicable fee to use Bright software products.
- iv. The Provider may change the terms and conditions of this agreement, and its privacy policy, at any time. The Provider will make reasonable efforts to communicate any changes to the User via a notification in Bright software products, or by sending an email to the User, but it is up to the User to ensure that it regularly checks, reads, understands and agrees to the most recent version of this agreement, and the Provider's privacy policy, as it will be deemed to accept all changes if the User continues to access and use Bright software products.

2. Who this agreement is between;

This agreement is between:

- i. "the User" - the person or organisation authorised to use Bright software products.
- ii. "the Provider" - BrightHR Ltd, company registration number 9282467, Vat number GB927524217 and whose registered office is situated at The Peninsula, Victoria Place, Manchester, M4 4FB.

By entering into this agreement, both the User and the Provider agree to be bound by its terms.

3. How the User accepts this agreement, and when this agreement starts;

- i. The User accepts the terms and conditions of this agreement when they log into the system.
- ii. This agreement will continue until terminated in accordance with clause 16 below.
- iii. If the User is not willing to accept these terms and conditions and therefore decides not to enter into this agreement, it should contact the Provider and is not permitted to use Bright software products or any of the Services.

4. The User's rights to use Bright software products, its obligations and 'cooling off';

- i. If the User accepts this agreement and pays the relevant fees, then the Provider gives to the User the right to use Bright software products in the way described in this agreement, and in accordance with any service announcements, administrative messages, sales support literature, and other information from the Provider. The User must not use Bright software products in any other way.
- ii. The User shall only use Bright software products for internal business management Health and Safety and HR purposes, and shall input its own employee data information in order to assist it in managing that information. It is also authorised to allow its own employees to input their own information.
- iii. Bright software products enables the User to submit content which is then stored in a document library. Such content will, generally, comprise employee data information, and will include such matters as their forename, surname, start date and job title. The User retains ownership of any Intellectual Property Rights that it holds in that content. However, access to this information is dependent upon the User complying with these terms and conditions, and ensuring that the applicable fee has been paid in full. The Provider will use all reasonable endeavours to implement technical and appropriate security measures to protect the information from loss or damage.
- iv. The User cannot transfer its rights under this agreement to use Bright software products (or any of the Services) to any other person or organisation.
- v. The User must comply with all applicable laws in respect of its use of Bright software products, and the User must also ensure that the content of any data it inputs into Bright software products does not, and will not, result in any injury, damage or harm to the Provider or any third party (including, without limitation, defamation or breach of confidentiality). Such content must not

contain anything which is unlawful, obscene, indecent or immoral or which promotes or condones any illegal or unlawful activities. It is also a condition of use that the User does not upload content (for example music or videos) for which it does not hold the copyright.

- vi. The User acknowledges that although the Provider forms part of a group of companies whose core business is the offering of professional HR and Health and Safety advice, Bright software products are not a substitute for seeking any employment law or health and safety advice.
- vii. The User may purchase or subscribe to third party complimentary products or software services that integrate or work with Bright software products ("Additional Services"). It is The User's responsibility to decide whether or not to access and use the Additional Services, and if the User chooses to do so, it must agree to the separate applicable terms and conditions presented to it by the Provider, or the third party, for those Additional Services. If there is a conflict between any of the terms of this agreement and the Additional Services terms, then the Additional Services terms will prevail in relation to the User's use of the Additional Services. The Provider is not responsible for any issue with any third-party technology, information and/or services and will not be liable for those issues. The Provider may withdraw access to such third party technology, information or services via Bright software products at any time and without notifying the User.
- viii. If the User is an 'individual' within the meaning of the Consumer Credit Act 2006 then they are entitled to a 'cooling off' period. A User falls within the definition of an 'individual' and is thereby entitled to a 'cooling off' period, if they are (1) a natural person (i.e an individual) (2) a partnership consisting of two or three persons not all of whom are bodies corporate or (3) an unincorporated body of persons which does not consist entirely of bodies corporate and is not a partnership. The 'cooling off' period will entitle such a User to cancel their use of Bright software products and release them from any obligation to pay a fee, provided such notification is received by the Provider within 5 working days from when they accept the terms of this agreement and become a User. In those circumstances the User may become liable to pay the Provider a fee for the Services used, such fee to be agreed between the Provider and the User or accepted by the User at the point of purchase.

5. (a) No longer in use

5. (b) Setting up a Bright software products account on the basis of a fixed term contract;

- i. The Provider will give the User its sign-in details to enable it to use Bright software products (the “sign-in information”) as soon as the User has registered with the Provider and has accepted these terms and conditions of use.
- ii. Following registration, the Provider will provide access to Bright software products until either the User or the Provider end this agreement either in one of the ways set out in clause 18 or by virtue of the operation of the terms of the contract signed by the Provider and the User. If at any time the Provider charges the User an incorrect fee, then the Provider reserves the right to rectify its invoice and claim the correct payment from the User which the User agrees to pay.

6. Use of Bright software products;

- i. The User is solely responsible for obtaining and maintaining its internet and network connections and any associated connectivity problems are its own responsibility.
- ii. The Provider will take reasonable steps to make sure that Bright software products are free from viruses but it cannot guarantee this. The Provider recommends that the User operates with its own virus-protection software as the Provider cannot be held responsible for any loss or damage caused by any viruses or other harmful technology that may infect the User’s computer systems, data or other material owned by it.
- iii. The Provider cannot guarantee that Bright software products will be compatible with the User’s web browser or computer set-up or that the User’s access to Bright software products will be uninterrupted or error free (as this may on occasions be beyond the Provider’s control).
- iv. The User is responsible for controlling access to its own Bright software products account. The User should not allow anyone else to use its sign in information and the User should also change its password at regular intervals.
- v. From time to time the Provider may temporarily suspend access to Bright software products for maintenance, repairs or other reasons. The Provider will try to do this outside normal business hours and provide the User with notice in advance but this might not always be possible.

7. Adding Services to the User's Bright software products Account;

- i. To add Additional Services to Bright software products, the User must pay the applicable fee for each Additional Service in accordance with the terms and conditions of this agreement.
- ii. The User can add Services via its Bright software products customer account portal. If the User wishes to add Additional Services to its Bright software products account but experiences difficulty, then the User must contact The Provider and must forthwith cease the addition of such Additional Services until the Provider has successfully cured the difficulty. When adding an Additional Service to its Bright software products account, the applicable fee payable) will be amended to reflect such Additional Service(s). To discuss any Additional Services the User must contact The Provider via email, telephone or web chat.

8. (a) No longer in use

8. (b) Fees for those Users who pay on a fixed term contract;

- i. Fees for using Bright software products are set out in the contract, signed when the User agreed to purchase the Services or accepted by the User at point of purchase.

9. What happens if The User is in Default?

- i. If, at any time, the User is in breach of any term of this agreement, or if the Provider does not receive payment from it for the use of Bright software products (including, without limitation, any of the Services it has subscribed to receive), then without prejudice to any other right or remedy which the Provider may have, the Provider is entitled to suspend or limit the User's use and any employees' self - service use of Bright software products (including all Services). The Provider may at its sole discretion offer the User a grace period during the defaulted payment period and has the right to suspend the service at the end of this period if payment has not been made. The Provider will notify the User of any payment related defaults.
- ii. Any suspension of the User's use of Bright software products shall continue until such time that the breach in question has been remedied to the Provider's reasonable satisfaction and/or the

Provider have received payment from the User in full. Any failure by the User to remedy a breach of this agreement, or to pay any amount due to the Provider, shall (without prejudice to any other right or remedy which the Provider may have) entitle it to terminate this agreement in accordance with clause 18 below. The Provider will notify the User by email of any intention to terminate the agreement.

- iii. The User shall indemnify and hold harmless the Provider from and against all Claims and Losses arising from (a) a breach of any part of this Agreement which results in loss, damage, liability, injury to the Provider and/or its employees, consultants, or other representatives and third parties, (b) infringement of third party Intellectual Property Rights or third party losses by reason or arising out of the User's access and use of Bright software products outside of that expressly permitted by this Agreement, or (c) any information or other materials supplied to the Provider by the User within or outside the scope of this Agreement. "Claims" shall mean all demands, claims, proceedings, penalties, fines and liability (whether criminal or civil, in contract, tort or otherwise) and "Losses" shall mean all losses including without limitation financial losses, damages, legal costs and other expenses of any nature whatsoever.

10. Restrictions on The User's use of Bright software products;

- i. The User must not introduce any viruses or harmful technology to Bright software products.
- ii. The User must not try to gain unauthorised access to Bright software products or any underlying technology.
- iii. The User must not try to affect the availability of Bright software products to other registered users.
- iv. Except as expressly permitted in this agreement, the User must not give anyone else any right (of any kind) to use or benefit from Bright software products in any way, or provide Bright software products to others, unless others are entitled to use Bright software products within the User's business and are added to Bright software products as a user of the Service.
- v. The User must not use Bright software products to develop its own software. Specifically, the User must not use or copy all or any part of Bright software products 'graphical user interface', 'operating logic' or 'database structure' for it to be used as part of, or to develop, any software or other product or technology.
- vi. The User must not make any use of the Services which damages or is likely to damage the Provider's business or reputation, the

availability or integrity of Bright software products, or which causes or threatens to cause the Provider to incur any legal, tax or regulatory liability.

11. Support;

- i. The Provider aims to provide the User with 24-hour support 7 days a week through the self-help tools (although there may be times where the Provider is unable to do so for reasons outside its control). The Provider will also provide support by [email] or [telephone] during working hours Monday to Friday between the hours of 8am and 6pm GMT. In the event that the Provider is required to access the User's system to provide such support the User duly authorises such access.
- ii. The Provider reserves the right to change how it provides support to the User (and if any applicable charges will become payable) by posting a notification on Bright software products or emailing the User with details of the changes. The Provider will aim to give the User as much advance notice as possible of these changes.
- iii. The Provider will not at any time however, give the User technical support or other assistance for any hardware, third-party software or other equipment issue on which Bright software products have been installed.

12. Intellectual Property Rights;

- i. Although the User has the right to use Bright software products as described in clause 4, the User will not own any of the Intellectual Property Rights in Bright software products. The Provider (or the third party from whom the Provider obtains the rights if the Provider is not the owner) will continue to own the Intellectual Property Rights in Bright software products, including any software the Provider provides to replace all or part of Bright software products. The only rights the User will have to Bright software products are as set out in this agreement.
- ii. The Provider (or its licensors) owns the rights to Bright software products and any related logos or images. By allowing the User to use Bright software products, the Provider does not give the User ownership of any of those rights, logos or images.
- iii. The User undertakes not to use the Providers name or brand in any promotion or marketing or announcement without its prior written consent.

13. Obligations on The Provider;

(a) Whilst the Provider aims to provide uninterrupted use of Bright software products, this cannot be guaranteed. The Provider will not be responsible for any failure to perform its obligations under this agreement, in the event that it is prevented from providing a continuous service due to circumstances beyond its control. Wherever possible, the Provider will provide an advance warning notification on Bright software products or by email of any known or planned interruptions and the Provider will use its best endeavours to keep any interruption to as short as possible.

(b) The Provider gives no warranties to the User in respect of the following matters:

- i. That Bright software products will meet the User's own needs;
- ii. That the User will be able to use Bright software products in any particular way;
- iii. That the User will get particular outputs from Bright software products;
- iv. That the standard of the results the User derives from using Bright software products will meet a particular standard; or
- v. that, where the User uses the Provider's technical support services, the Provider will be able to correct or remedy the User's particular problem

(c) The User cannot rely on any statement or representation made by any party prior to the registration of the User as a user of Bright software products.

(d) The Provider agrees that it will use its reasonable skill and care to provide the Services to the User under this agreement.

14. Providers Responsibilities;

(a) The Providers liability in contract, tort (including negligence or breach of statutory duty), misrepresentation, restitution or otherwise arising under or in connection with this agreement will be limited to an amount equal to the total of all fees paid or payable by the User for its use of Bright software products in the 1-month period in which the claim

arose.

(b) The Provider will not be responsible, whether in contract, tort (including negligence or breach of statutory duty), misrepresentation, and restitution or otherwise for any of the following (even if the Provider knew or should have known there was a possibility the User could suffer or incur such loss or damage):

- i. Loss of profit;
- ii. Loss of business or revenue;
- iii. Depletion of goodwill or similar losses;
- iv. Loss of use or loss of or damage to data/information inputted by the User into Bright software products;
- v. Any interruption to the User's business or damage to information, however that interruption or damage is caused;
- vi. Any loss or damage which the Provider could not have reasonably foreseen at the time the User entered into this agreement including, without limitation, any special, indirect or consequential loss or damage.

(c) Nothing in this agreement will exclude or limit the liability of either the User or the Provider in respect of:

- i. Fraud
- ii. Death of or personal injury to any person as a result of negligence
- iii. Any other matter which cannot be excluded or limited under applicable law including the European Union or a member state of the European Union.
- iv. Any infringement of the General Data Protection Regulation 2016/679 (GDPR)

15. Force Majeure;

Neither party shall be liable for any default arising due to act of God, war, any industrial action including strike and lockout, fire, flood, drought, tempest or other natural disaster, or any other event beyond either party's reasonable control.

16. Termination;

(a) No longer used

(b) Termination of an agreement based on a fixed term contract.

- i. The termination provisions in the contract or terms accepted by the User at point of purchase are repeated and set out herein.

(c) Termination generally;

- i. If either the User or the Provider discover that there has been a breach of the terms of this agreement by then it can:-
 - i. Require the party in breach by notice in writing to rectify it within 30 days of the date of service of such notice.
 - ii. If the breach is not rectified within that period to terminate this agreement by giving written notice that this agreement will terminate forthwith.

- ii. If either party shall;

- i. become insolvent or bankrupt or
- ii. have a receiving order or administration order made against it or compound with its creditors, or
- iii. being a corporation commences to be wound up (not being a member's voluntary winding up for the purposes of reconstruction or amalgamation), or
- iv. carries on its business under an administrator or administrative receiver for the benefit of its creditors or any of them then the other party shall have the right forthwith by notice in writing to that party or to the administrator, administrative receiver or to the liquidator or to any person in whom this agreement shall have become vested to terminate this agreement, to terminate this agreement.

- iii. No matter how this agreement ends, the information the User stores in Bright software products remains the User's information and the User can access it in a format provided by Bright software products before the end of the agreement. After this agreement ends, the information the User may have stored in Bright software products will be retained for a period of 6 years.

17. Miscellaneous;

1. If any provision of this Agreement is held illegal or unenforceable such provision shall be severed and shall be inoperative, and, provided that

the fundamental terms and conditions of this agreement remain legal and enforceable, the remainder of this agreement shall remain operative and binding on the Parties

- i. If the User or the Provider fails to, or delays in, exercising any rights under this agreement, that will not mean that those rights cannot be exercised in the future.
- ii. This agreement and the documents the Provider refers to above (including the contract for those users who use Bright software products by virtue of that written contract) constitute is the entire agreement between the User and the Provider for use of Bright software products, and replaces all documents, information and other communications (whether spoken or written) between them for such use.
- iii. This agreement is personal to the User and may not be transferred, assigned, subcontracted, licensed, charged or otherwise dealt with or disposed of (whether in whole or in part) by the User without the Provider's prior written consent. The Provider may transfer, assign, subcontract, license, charge or otherwise deal with or dispose of (whether in whole or in part) this agreement at any time without the User's consent.
- iv. A person who is not a party to this agreement has no right to enforce any term of it.
- v. Where either party is required to notify the other party by email, the party shall be deemed to have received the email on the first business day following transmission.

18. Which laws govern this agreement?

1. If the User subscribes to Bright software products in the United Kingdom, then this agreement (and all non-contractual claims and disputes) is governed by the laws of England and Wales and the User and the Provider both agree that the courts of England and Wales shall be the only courts competent to decide disputes in relation to this agreement.

19. Disclaimer;

The Furlough Navigator is a tool to assist employers with their submission of information to HMRC in respect of any furloughed workers. The Furlough Navigator tool is based on guidance published by the Government on its website (www.gov.uk) which is regularly being updated.. The information provided by BrightHR Limited in relation to the Coronavirus Job Retention Scheme does not amount to 'advice' and Bright HR Limited does not accept any liability or responsibility for the

submission or accuracy of information provided to HMRC. All claims submitted to HMRC remain the sole responsibility of the employer.

Privacy

This privacy policy explains how we collect and use any personal information we collect about you. The policy depends on whether you are "The User" (person or organisation authorised to use BrightHR), an Employee of "The User" or a Visitor to the website.

Privacy Notice for Website Visitors

This privacy policy explains how personal data is collected and used when you use our websites. It also explains how we process any data that you supply to us on this website, for instance to request a quote or to use our online services.

BrightHR is the Data Controller for any personal data that you supply to us during your visit to our website.

Our address is

BrightHR Ltd
The Peninsula
Victoria Place
Manchester
M4 4FB

Telephone 0844 892 3928

Email gdpr@brighthr.com

What personal data we collect

The personal data collected depends on how you use our website. You can browse the site, you can fill in forms on the website to request information or quotes from us, download documents from us, or you can subscribe to our emails, and other activities. Our website collects personal data to provide these services.

We collect information about you when you visit our website; subscribe to our newsletters or to receive our publications; apply for employment with us; attend one of our seminars; and engage in business dealings with us.

What we do with your personal data

When you visit our website, a record of your visit is made. This data includes your device's IP address. That data is used completely anonymously, in order to determine the number of people who visit our website and the most frequently used sections of the site. This enables us to continually update and refine the site. If you use any forms on the website to send an email to us, a record will also be made of your email address and your telephone number.

The following table sets out how we handle your personal data and our legal basis for doing so under GDPR and the Data Protection Act 2018.

What we do	Our legal basis under GDPR
Use the personal data that you provide on our web forms and questionnaires	Article 6(1)(b) - when you provide us with your personal data, for instance to obtain a quote for our services, this is a necessary step to take at the request of the data subject prior to entering into a contract
Provide our online services platforms - Bright HR, or hronline,	Article 6(1)(b) - this is necessary for the performance of a contract with you, our data subject
Contact you regarding the services we provide	Article 6(1)(f) - we need to contact you for our legitimate interests so that we can gather more information for the provision of our services, or to deliver those services most effectively
Retain your data under our data retention policy after your contract has expired	Article 6(1)(f) - we need to retain your personal data for only as long as necessary under the law to protect our legitimate interests
Where you require us to make Reasonable Adjustments to enable you to attend a meeting or interview, we may require further information from you.	Article 9(2)(a) of GDPR (explicit consent). If this includes information about your physical or mental health, such information (being sensitive personal data, Special Category

data), will only be used by us, with your explicit consent, to assess your eligibility for Reasonable Adjustments. We will not share or disclose it to others.

You can withdraw your consent as anytime by contacting us. Please note that we may not be able to process your request for Reasonable Adjustments if you do this.

The following table sets out the categories of personal data that we obtain.

Personal Data

Name, postal address, email address, website, identification number, location data, online identifier - these are classed as personal data

Explanation

This data is provided by you on our web forms and questionnaires, either to obtain a quote from us, subscribe to one of our newsletters, request a service from us or as part of the provision of your existing contractual services.

This data may be provided if you apply for a job opportunity.

We may collect, hold, use and disclose the information collected to compile statistical data and to; maintain our database; develop/improve our website; respond to any email enquiries; notify you of any upcoming marketing, training or other events that you have opted in to; provide you with publications; manage quality control; manage systems administration; attend to compliance issues; provide you or your organisation with advice and determine suitability for employment.

We will not use or disclose your personal information for any other purpose which is not related (or in the case of sensitive information, directly related) to the above purposes without your consent, unless otherwise authorised, required or permitted under the laws of England and Wales. The Group does not sell your data to third parties.

If you no longer wish to receive information about our services, please send an email to our Data Protection and Compliance Officer (gdpr@brighthr.com) advising that you do not wish to receive further information.

Will we disclose your data?

Personal data will only be disclosed on a confidential basis to external service providers so that they can provide services such as financial or administrative services in connection with the operation of our business; and to any person (where necessary) in connection with their services, such as law enforcement, regulatory authorities, partners or advisors; or to companies within the Peninsula Group in the UK.

The handling of these operations is governed by a data processing contract between us and our external service provider, ensuring a commitment to the principals of the GDPR and the Data Protection Act 2018. We ensure external service providers are only authorised to use personal data for the limited purposes specified in our agreement with them.

How long we keep your personal data

Personal data from our data subjects is retained in line with our data retention policy. The Group keeps most data for 7 years, which covers the 6 years by law in which we have to keep certain information for a minimum of 6 years plus the current year. Personal data that is no longer necessary to be kept under the Group's data retention policy will be deleted. Under the Group's data retention policy, there are certain exemptions in relation to financial data and health data. A copy of the Group's data retention policy can be made available upon request.

Your Rights

You have the following rights in relation to personal data held on you by the Group:

- The right to be informed about how personal data is used - (this notice)
- The right to access a copy of personal data that the Group holds about you
- The right to rectification of any errors in personal data held by the Group
- The right to erasure of any personal data
- The right to restrict processing
- The right to data portability

- The right to object
- Rights in relation to automated decision making including profiling

If you wish to learn more about these rights and how they operate, please look at the ICO's website <https://ico.org.uk/for-the-public/>.

BrightHR does not operate any automated decision making systems.

You have a right to request a copy of the personal data that we hold about you. If you would like a copy of some or all of your personal data please email gdpr@brighthr.com or write to our Data Protection and Compliance Officer at The Peninsula, Victoria Place, Manchester, M4 4FB. Proof of your identity will be required for security purposes.

If you are unhappy with the response that you receive from us when you exercise your GDPR rights or Data Protection Act 2018 rights, you have the right to lodge a complaint to the ICO. More guidance about raising a complaint with us is available on the ICO's website <https://ico.org.uk/for-the-public/raising-concerns/> and for raising a complaint with the ICO, more information is available on <https://ico.org.uk/concerns/>.

Cookies

This website uses Google Analytics, a web analytics service provided by Google, Inc. Google Analytics sets a cookie in order to evaluate your use of this website and compile reports for us on activity on the website. Google stores the information collected by the cookie on servers in the United States and the transfer of the data to servers in the USA is governed by the EU-US Privacy Shield framework. Google may also transfer this information to third parties where required to do so by law, or where such third parties process the information on Google's behalf. Google will not associate your IP address with any other data held by Google. By using this website, you consent to the processing of data about you by Google in the manner and for the purposes set out above. More information about Google's compliance with GDPR can be obtained from their website <https://privacy.google.com/businesses/compliance>.

Cookies are text files placed on your computer to collect standard internet log information and visitor behaviour information. This information is used to track visitor use of the website and to compile statistical reports on website activity. For further information visit www.aboutcookies.org.



You can set your browser not to accept cookies and the above websites tell you how to remove cookies from your browser. However, in a few cases some of our website features may not function as a result.

Other websites

Our website may contain links to other sites. This privacy policy only applies to this website so when you link to other websites you should read their own privacy policy.

How to contact us

Please review the website regularly as this statement may change from time to time. If you have any questions about our privacy policy or information we hold about you please contact:

Data Protection and Compliance Officer

Telephone 0844 892 2779

Email gdpr@brighthr.com

Privacy Notice for Customers

In accordance with the General Data Protection Regulation (GDPR), BrightHR have implemented this privacy information notice to inform you, our current and former clients, of the types of data we process about you. We also include within this notice the reasons for processing your data, the lawful basis that permits us to process it, how long we keep your data for and your rights regarding your data.

This notice applies to current and former clients.

We are a Data Processor of the personal data that you supply to us under your contract with us.

A. DATA PROTECTION PRINCIPLES

Under GDPR, all personal data obtained and held by us must be processed according to a set of core principles. In accordance with these principles, we will ensure that:

- a. processing is fair, lawful and transparent
- b. data is collected for specific, explicit, and legitimate purposes
- c. data collected is adequate, relevant and limited to what is necessary for the purposes of processing
- d. data is kept accurate and up to date. Data which is found to be inaccurate will be rectified or erased without delay
- e. data is not kept for longer than is necessary for its given purpose
- f. data is processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures
- g. we comply with the relevant GDPR procedures for international transferring of personal data

B. TYPES OF DATA HELD

We keep several categories of personal data on and from our clients in order to carry out effective and efficient processes. We hold the data within our computer systems to provide our advice service and case management systems.

Specifically, we hold the following types of data:

- a. personal details such as name, address, phone numbers, job title, email addresses etc for the main contact and other contacts for the delivery of the service
- b. IT service use including online service access records.

C. COLLECTING YOUR DATA

You provide several pieces of data to us directly when the contract is signed, during the on boarding process and during the contract and after the contract has ended.

Personal data is kept in within the Company's secure systems.

D. LAWFUL BASIS FOR PROCESSING

The law on data protection allows us to process your data for certain reasons only. In the main, we process your data in order to comply with a legal requirement or in order to effectively manage the service contract we have with you, including ensuring we can deliver the service to you.

The information below categorises the types of data processing we undertake and the lawful basis we rely on.

Activity requiring your data	Lawful basis
Set up your account	Performance of the contract
Carry out the delivery of the services you have on your account	Performance of the contract
Ensuring payments are made under your account	Performance of the contract
Ensuring VAT and insurance premium tax is paid	Legal obligation
Carrying out checks in relation to your company status and validating the information supplied to us	Legal obligation
Making financial decisions in relation to entering both initial and subsequent contracts	Our legitimate interests
Making decisions about service delivery methods	Our legitimate interests
Ensuring efficient administration of contractual services to you	Our legitimate interests
Effectively monitoring the service provided including adherence to commitments and service entitlements	Our legitimate interests
Maintaining up to date records about you to ensure, amongst other things, effective correspondence can be achieved and appropriate contact points in place	Our legitimate interests
Dealing with legal claims made against us	Our legitimate interests
Preventing fraud	Our legitimate interests

Ensuring our administrative and IT systems are secure and robust against unauthorised access

Our legitimate interests

E. FAILURE TO PROVIDE DATA

Your failure to provide us with data may mean that we are unable to fulfil our requirements for entering into a contract with you. This could include being unable to offer you services or administer existing contractual services.

F. WHO WE SHARE YOUR DATA WITH

All employees within Brighthr that handle your personal data are trained in ensuring data is processed in line with GDPR.

Data is shared with other companies within the Peninsula Group of Companies. Brighthr is a company within the Group. Data may be shared for the following reasons: administration of services specifically supplied by Group subsidiaries. For example, Peninsula/Croner provides employment and health and safety services. Your data is shared with GROUP companies to facilitate the delivery of all the services you are contracted to receive.

Your data is not shared with third parties, except for other reasons to comply with a legal obligation placed upon us. We have a data processing contract in place with such third parties to ensure data is not compromised. Third parties must implement appropriate technical and organisational measures to ensure the security of your data.

We may share your data with bodies outside of the European Economic Area. These countries are Canada, Australia, New Zealand (and from March 2019: the United Kingdom) and the reason for sharing with these countries is to facilitate our legitimate business interests in providing you with the contracted services where the BUSINESS employees responsible for the provision of the service are based outside the EEA. We have put the following measures in place to ensure that your data is transferred securely and that the bodies who receive the data that we have transferred process it in a way required by EU and UK data protection laws:

The data processing systems in use at other companies within the BUSINESS have comparable levels of security and safety to the systems in operation in countries within the European Economic Area.

G. PROTECTING YOUR DATA

We are aware of the requirement to ensure your data is protected against accidental loss or disclosure, destruction and abuse. We have implemented processes to guard against such.

H. RETENTION PERIODS

We only keep your data for as long as we need it for, which will be at least for the duration of your service contract plus 7 years from the date that service contract with us terminates, although in some cases we will keep your data for a longer period after your contract has ended. Some data retention periods are set by the law. Retention periods can vary depending on why we need your data, as set out below:

Record	Recommended Retention Period
Assessments under health and safety regulations and records of consultations with safety representatives and committees	Permanently
HMRC approvals	Permanently
Money purchase details	6 years after transfer or value taken
Health data	30 or 50 years
Litigation cases	7 years from the conclusion of the litigation case
All other data	7 years from the date the service contract with us terminates

I. AUTOMATED DECISION MAKING

Automated decision making means making decision about you using no human involvement e.g. using computerised filtering equipment. No decision will be made about you solely on the basis of automated decision making (where a decision is taken about you using an electronic system without human involvement) which has a significant impact on you.

J. CLIENT RIGHTS

You have the following rights in relation to the personal data we hold on you:

- a. the right to be informed about the data we hold on you and what we do with it;
- b. the right of access to the data we hold on you. More information on this can be found in the section headed "Access to Data" below and in our separate policy on Subject Access Requests";
- c. the right for any inaccuracies in the data we hold on you, however they come to light, to be corrected. This is also known as 'rectification';
- d. the right to have data deleted in certain circumstances. This is also known as 'erasure';
- e. the right to restrict the processing of the data;
- f. the right to transfer the data we hold on you to another party. This is also known as 'portability';
- g. the right to object to the inclusion of any information;
- h. the right to regulate any automated decision-making and profiling of personal data.

K. CONSENT

Where you have provided consent to our use of your data, you also have the right to withdraw that consent at any time. This means that we will stop processing your data.

L. MAKING A COMPLAINT

If you think your data rights have been breached, you are able to raise a complaint with the Information Commissioner (ICO). You can contact the ICO at Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF or by telephone on 0303 123 1113 (local rate) or 01625 545 745.

M. DATA PROTECTION COMPLIANCE

Our Data Protection and Compliance Officer is:

Gail Tuck

Telephone 0844 892 2779

Email gdpr@brighthr.com

Privacy Notice for User's Employees

In accordance with the General Data Protection Regulation (GDPR), BrightHR have implemented this privacy notice to inform you, our user's employee, of the types of data we process about you. We also include

within this notice the reasons for processing your data, the lawful basis that permits us to process it, how long we keep your data for and your rights regarding your data. **We are a data processor and your employer remains the data controller at all times. Your data may have been provided to us by the data controller or by you as the data subject.**

This notice applies to users of the Brighthr software who are employees of our Users.

A. DATA PROTECTION COMPLIANCE

Our Data Protection Officer can be contacted at:

Brighthr, The Peninsula, Victoria Place, Manchester, M4 4FB.

Telephone: 0808 145 3490

Email: gdpr@brighthr.co.uk

B. DATA PROTECTION PRINCIPLES

Under GDPR, all personal data obtained and held by us must be processed according to a set of core principles. In accordance with these principles, we will ensure that:

- a. processing is fair, lawful and transparent
- b. data is collected for specific, explicit, and legitimate purposes
- c. data collected is adequate, relevant and limited to what is necessary for the purposes of processing
- d. data is kept accurate and up to date. Data which is found to be inaccurate will be rectified or erased without delay
- e. data is not kept for longer than is necessary for its given purpose
- f. data is processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures
- g. we comply with the relevant GDPR procedures for international transferring of personal data

C. TYPES OF DATA HELD

We may keep several categories of personal data about you in order to allow you to use the software. We keep this data within our secure computer systems.

Specifically, we may hold the following types of data:

1. Name
2. Address

3. Date of Birth
4. Job title
5. Contact details, for example, details of next of kin
6. Immigration status details i.e. passport number/visa number and expiry dates
7. National Insurance Number
8. Documents your employer uploads
9. If you are a BrightHR user, information relating to employment, i.e. absence records, development records and annual leave entitlement, sickness records, working pattern records and shift and rota patterns.
10. If you are a BrightSafe user information relating to health and safety i.e. accident records, your role in managing health and safety.

D. LAWFUL BASIS FOR PROCESSING

The law on data protection allows us to process your data for certain reasons only. We process your data for our legitimate interests in order to provide you access to and use of the software and to provide insights to your employer in order to help them manage their obligations to you as an employee. We may also process personal data in connection with the establishment, exercise or defence of legal claims.

E. WHO WE SHARE YOUR DATA WITH

Employees within our company who have responsibility for the provision of technical support services may have access to your data which is relevant to their function to allow them to provide technical support services to you or your employer. All employees with such responsibility have been trained in ensuring data is processed in line with GDPR.

We may share your data with third parties to comply with a legal obligation upon us.

We will not share your data with bodies outside of the European Economic Area.

F. PROTECTING YOUR DATA

We are aware of the requirement to ensure your data is protected against accidental loss or disclosure, destruction and abuse. We have implemented processes to guard against such.

G. RETENTION PERIODS

We only keep your data for as long as we need it for, which will be at least for the duration of your employer's contract with us for the provision of the service.

H. AUTOMATED DECISION MAKING

Automated decision making means making decision about you using no human involvement e.g. using computerised filtering equipment. No decision will be made about you solely on the basis of automated decision making (where a decision is taken about you using an electronic system without human involvement) which has a significant impact on you.

I. INDIVIDUAL'S RIGHTS

You have the following rights in relation to the personal data. However if you wish to exercise your rights any request should be made to your employer as the data controller. Any request made to us as the data processor will be forwarded to our data controller.

- a. the right to be informed about the data we hold on you and what we do with it;
- b. the right of access to the data we hold on you.
- c. the right for any inaccuracies in the data we hold on you, however they come to light, to be corrected. This is also known as 'rectification';
- d. the right to have data deleted in certain circumstances. This is also known as 'erasure';
- e. the right to restrict the processing of the data;
- f. the right to transfer the data we hold on you to another party. This is also known as 'portability';
- g. the right to object to the inclusion of any information;
- h. the right to regulate any automated decision-making and profiling of personal data.

J. CONSENT

Where you have provided consent to our use of your data, you also have the right to withdraw that consent at any time. This means that we will stop processing your data.

K. MAKING A COMPLAINT

If you think your data rights have been breached, you are able to raise a complaint with the Information Commissioner (ICO). You can contact the ICO at Information Commissioner's Office, Wycliffe House, Water Lane,

Wilmslow, Cheshire SK9 5AF or by telephone on 0303 123 1113 (local rate) or 01625 545 745.

Data Security

Data Protection Statement of Bright HR which is owned and operated by Bright HR Limited

We will use the personal data provided to us only for its intended purpose, and in accordance with Data Protection Law.

Security

We are committed to ensuring that employee information is kept secure at all times, and we will implement appropriate technical and organisational measures against the unauthorised or unlawful disclosure of such information, and so as to prevent its accidental loss, destruction or damage.

Personal access to Bright Software Products will only be via a secure username and password. The username and password for each individual is unique and only allows access to their own personal information. Only certain authorised staff, who are required to have access to the personal information of other employees for the purposes of their job role, will be authorised and will have the necessary access rights to do so. They will receive relevant training and will be asked to agree to abide by the terms of this Data Protection Statement.

All users of Bright Software Products should keep their unique user and password strictly confidential. Users of Bright Software Products must notify us if they become aware of any unauthorised access, and we will notify clients of Bright Software Products should we become aware of any security breach involving loss, corruption or theft of employee information.

Storage and Encryption

By leveraging the benefits of Cloud Computing all Bright Software Products data is stored on highly secure systems. These utilise the latest encryption and security technologies which are ISO/IEC 27001:2013, ISO/IEC 27017:2015 and ISO/IEC 27018 compliant. To maintain our PCI compliance, approved independent security vendors are used by BrightHR to ensure all our systems are scanned for any vulnerabilities.

Data Processing

BrightHR will only process personal data in accordance with the User's instructions, the User retains the responsibilities of the data controller and determines the purposes and means of processing personal data.

1. During Processing the Provider shall

- a. comply with the General Data Protection Regulation and the Data Protection Act 2018;
- b. only process the Personal Data for the purposes of performing its obligations under this Agreement and in accordance with the written instructions given by the User from time to time, unless the party is subject to an obligation under applicable law (including Data Protection Law) of the European Union or a member state of the European Union to do otherwise, in which case the party shall (unless prohibited by law) notify the User in advance of that legal obligation;
- c. notify the User immediately if an instruction from the User breaches a requirement of Data Protection Law;
- d. not disclose the Personal Data to any third party in any circumstances other than on the User's written instructions, with the User's specific written consent or where required to do so by applicable law (including (without limitation) Data Protection Law);
- e. with respect to the Personal Data taking 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 natural persons, implement and maintain appropriate technical and organizational measures to ensure a level of

security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1)(a), (b), (c) and (d) of the GDPR, and the measures shall, at a minimum, comply with the requirements of Data Protection Law, including Article 32 of the GDPR;

- f. ensure that all personnel with access to Personal Data:
 - i. are subject to a contractual duty of confidence to hold the Personal Data in strict confidence;
 - ii. only process the Personal Data in the manner permitted by this Schedule;
- g. at the User's request, provide the User with such assistance as is contemplated by Article 28(3)(f) of the GDPR;
- h. immediately notify the User in writing of each Security Incident of which it becomes aware;
- i. assist the User with all data subject rights requests received from data subjects of the Personal Data, including (without limitation) by providing to the User such assistance as is contemplated by Article 28(3)(e) of the GDPR;
- j. if it receives any complaint, notice, request (including any subject access request) or communication (whether from a data subject, data protection regulator or other person) which relates directly or indirectly to the processing of Personal Data or to either party's compliance with Data Protection Law, it shall immediately notify the User in writing and it shall provide the User with full cooperation and assistance in relation to the same, and shall not respond to the complaint, notice, request or communication without the prior written consent of the User (except to the extent required by law), provided that the Supplier may acknowledge receipt;
- k. not transfer access or process the Personal Data outside the EEA save where expressly authorised or instructed by the User in writing to do so;
- l. not subcontract the processing of Personal Data to a sub-processor without the prior written consent of the User and in the event that the User provides its consent, the party shall (prior to the sub-processor processing the Personal Data) enter into an agreement with the sub-processor on terms that provide no less protection for the Personal Data than those set out in this Schedule and meet the requirements of Data Protection Law, and the party shall remain fully liable for the acts and omissions of each sub-processor; The processor shall notify the controller concerning the addition

or replacement of sub-processors in advance and allow the controller to raise any objections to such changes

- m. at the User's option, securely return to the User or securely destroy the Personal Data, together with all copies in any form and in any media, in the party's power, possession or control promptly following the earlier of:
 - i. termination or expiry of this Agreement;
 - ii. a request from the User; or
 - iii. if the party no longer needs the Personal Data in connection with the performance of its obligations under the Agreement;
- n. provide the User with all information requested by the User to enable the User to verify the party's (and each sub-processor's) compliance with this Schedule;
- o. on request supply the User with written confirmation that all facilities, premises, equipment, systems, documents and electronic data used for the processing of Personal Data by the party are compliant with the GDPR and assist with any audit that may be required.

2. Data Processing Details

(a)	Subject matter, nature and purpose of the processing of Personal Data under this Agreement	Subject matter The provision of online human resource management tools and other information services and materials. Nature Processing activities, such as storage, retrieval, analysing, data collection and data transfer will all be undertaken by the Supplier. Purpose Personal Data is processed in order to enable the Supplier to provide access to the services to the Authorised Users of the User, to provide insights to your employer in order to help them manage
-----	---	---

your employment and for administration of the contract and the services.

(b) **Duration of the processing of Personal Data under this Agreement**

For the term of this Agreement.

(c) **Type of Personal Data processed under this Agreement**

Personal Data

- Name
- Address
- Date of Birth
- Job title
- Contact details, for example, details of next of kin
- Immigration status details i.e. passport number/visa number and expiry dates
- National Insurance Number
- If you are a BrightHR user information relating to employment, i.e. absence records, development records and annual leave entitlement. This information may be collected via application for employment forms, personal details forms, personnel files and records and any subsequent amendments to such documents.
- If you are a BrightSafe user information relating to health and safety i.e. accident records, your role in managing health and safety.