

Privacy Policy – Employee Personal Data

This Privacy Policy deals only with our handling of our Employees' and ex-employees' data as a Controller of the data we hold for our own purposes on our systems and for the reasons set out in the Schedule at the end of this Privacy Policy

This privacy policy does not cover our handling of any other data as a Controller of the data we hold for our own purposes on our systems which is dealt with in a separate Privacy Policy which can be found [here](#).

This Privacy does not cover our handling of our Customers' data in their own instance on Hornbill for which they are the Controller and we are the Processor. Our legal obligations as a Processor are set out in our Terms of Service and Subscription Agreements which can be found [here](#).

This Privacy Policy does not cover the Processing of our SupportWorks Customers' data when we are providing support and consultancy services. Our legal obligations as a Processor in those circumstances are set out [here](#).

Although the UK has left the European Union Hornbill will continue to follow the principles set out in GDPR as enacted into UK Law by the DPA. Accordingly this Privacy Policy still refers to GDPR.

DEFINITIONS

'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

'DPA' means the Data Protection Act 2018

'GDPR' means REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016. The full text of the GDPR can be found here <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&fromen>

'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, 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

DATA CONTROLLER

Hornbill Corporate Limited is the ultimate holding company for the following Hornbill Group companies:

- Hornbill Technologies Limited
- Hornbill Service Management Applications Limited

- Hornbill Service Management Limited

This privacy policy is applied consistently across these companies and the single point of contact for enquires about privacy is the CFO who can be contacted at data.privacy@hornbill.com. The CFO can be contacted by post at Hornbill Corporate Limited, Apollo, Odyssey Business Park, West End Road, Ruislip, HA4 6QD UK.

If you are in the EEA, you may address privacy-related inquiries to our EU representative pursuant to Article 27 GDPR:

EU-REP.Global GmbH, Attn: Hornbill, Hopfenstr. 1d, 24114 Kiel, Germany

hornbill@eu-rep.global

www.eu-rep.global

YOUR RIGHTS

All individuals for whom we hold personal data have the following rights and our systems and processes will ensure that these rights are respected:

1. Right to be Informed
2. Right of Access
3. Right to Rectification
4. Right to Erasure
5. Right to Restrict Processing
6. Right to Data Portability
7. Right to Object
8. Rights in Relation to Automated Decision Making

These rights and our policies to ensure they are respected are considered in more detail in the following sections.

RIGHT TO BE INFORMED

Hornbill will inform all individuals about whom it holds personal data the following:

1. What is the purpose for which the data has been collected?
2. What is the lawful basis on which we process the data?
3. What categories of data are obtained and how do we ensure that only data that is needed for the purpose is collected?
4. Who are the recipients of the data, if any?
5. Which countries will we transfer the data to?
6. Where did we get the data from?
7. How do we ensure that the data is kept accurate and up to date?
8. How do we ensure that inaccuracies are corrected?
9. How do we ensure that data that is no longer required for the purpose for which it is collected is deleted?
10. How do we ensure that the data is secure?

Hornbill will provide these details to you at the first time we collect the personal data from you if we collect the data directly from you.

Hornbill will provide these details no more than one month after first obtaining the personal data if we have not collected it from you.

We will provide the details in a concise, transparent, intelligible, easily accessible way that uses clear and plain language.

This information is provided in Schedule 1.

RIGHT OF ACCESS

If you have been informed by Hornbill that we Process your personal data you have the right to access your data so that you are aware of and can verify the lawfulness of the Processing Hornbill are doing.

Upon your request to Hornbill at the email or postal address given above Hornbill will provide you a copy of your data within one month.

Prior to releasing any data to you Hornbill will need to verify your identity using reasonable means.

Wherever possible Hornbill will make the data available to you in electronic format by means of a shared document.

Hornbill will provide a copy of the information free of charge. However, Hornbill may charge a reasonable fee when a request is manifestly unfounded or excessive, particularly if it is repetitive.

Hornbill may also charge a reasonable fee to comply with requests for further copies of the same information. This does not mean that Hornbill will charge for all subsequent access requests.

The fee will be based on the administrative cost of providing the information and you will be notified of it in advance of Hornbill providing your data. If Hornbill charges a fee Hornbill will not comply with the request until we have received the fee.

Hornbill may extend the period of compliance by a further two months where requests are complex or numerous. If this is the case, Hornbill will inform you within one month of the receipt of the request and explain why the extension is necessary.

Where requests are manifestly unfounded or excessive, in particular because they are repetitive, Hornbill may as an alternative to charging a fee refuse to respond. Where Hornbill refuses to respond to a request, Hornbill will explain why to you. Hornbill will also inform you of your right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

RIGHT OF RECTIFICATION

You have the right to have any personal data we Process corrected if it contains errors.

If the personal data contains errors you should provide Hornbill with written arguments and evidence to clearly identify the errors for Hornbill.

Upon your request to Hornbill preferably at the email or postal address given above Hornbill will take reasonable steps within one month to satisfy itself that the data is accurate and to rectify the data if necessary. Hornbill will consider the arguments and evidence provided by you.

What steps are reasonable will depend on the nature of the personal data and what it will be used for. The more important it is that the personal data is accurate, the greater the effort Hornbill will put into checking its accuracy and, if necessary, taking steps to rectify it. For example, Hornbill will make a greater effort to rectify inaccurate personal data if it is used to make significant decisions that will affect an individual or others, rather than trivial ones.

It is also complex if the data in question records an opinion. Opinions are, by their very nature, subjective, and it can be difficult to conclude that the record of an opinion is inaccurate. As long as the record shows clearly that the information is an opinion and, where appropriate, whose opinion it is, it may be difficult to say that it is inaccurate and needs to be rectified.

Hornbill will in any event restrict the processing of the personal data in question whilst we are verifying its accuracy.

Hornbill will let you know if we are satisfied that the personal data is accurate, and tell you that you will not be amending the data. Hornbill will explain our decision, and inform you of your right to make a complaint to the ICO or another supervisory authority; and your ability to seek to enforce their rights through a judicial remedy.

Hornbill will place a note on our systems indicating that you have challenged the accuracy of the data and your reasons for doing so.

Hornbill may refuse to comply with a request for rectification if the request is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature.

If Hornbill considers that a request is manifestly unfounded or excessive Hornbill may:

- request a reasonable fee to deal with the request; or
- refuse to deal with the request.

In either case Hornbill will justify our decision to you.

Hornbill will base the reasonable fee on the administrative costs of complying with the request. If Hornbill decides to charge a fee Hornbill will contact you without undue delay and within one month. Hornbill will not comply with the request until we have received the fee.

If Hornbill refuses to comply with a request for rectification we will inform you without undue delay and within one month of receipt of the request about:

- the reasons we are not taking action; and
- your right to make a complaint to the ICO or another supervisory authority; and
- your ability to seek to enforce this right through a judicial remedy.

Hornbill will also provide this information if we request a reasonable fee or need additional information to identify you.

A request to rectify personal data does not need to mention the phrase 'request for rectification' or Article 16 of the GDPR to be a valid request. As long as you have challenged the accuracy of your data and have asked Hornbill to correct it, or have asked that Hornbill take steps to complete data held about you that is incomplete, this will be a valid request under Article 16 of GDPR.

This presents a challenge as any of our employees could receive a valid verbal request. Hornbill has a legal responsibility to identify that you have made a request to us and handle it accordingly. Hornbill will consider which of our staff who regularly interact with individuals may need specific training to identify a request.

Hornbill will record details of the requests we receive, particularly those made by telephone or in person. Hornbill will check with you that we have understood your request, as this can help avoid later disputes about how we have interpreted the request. Hornbill will keep a log of verbal requests.

Hornbill may extend the time to respond by a further two months if the request is complex or Hornbill have received a number of requests from you. Hornbill will let you know without undue delay and within one month of receiving your request and explain why the extension is necessary.

The circumstances in which Hornbill can extend the time to respond can include further consideration of the accuracy of disputed data - although Hornbill will only do this in complex cases - and the result may be that at the end of the extended time period Hornbill expects to inform you that Hornbill considers the data in question to be accurate.

If Hornbill has doubts about the identity of the person making the request Hornbill will ask for more information. Hornbill will only request information that is necessary to confirm who you are. The key to this is proportionality. Hornbill will take into account what data it holds, the nature of the data, and what we are using it for.

Hornbill will let you know without undue delay and within one month that we need more information from you to confirm your identity. Hornbill will not comply with the request until we have received the additional information.

If Hornbill has disclosed the personal data to others, Hornbill will contact each recipient and inform them of the rectification or completion of the personal data - unless this proves impossible or involves disproportionate effort. If you ask us to, Hornbill will also inform you about these recipients.

RIGHT TO ERASURE

Under Article 17 of the GDPR YOU have the right to have personal data erased. This is also known as the 'right to be forgotten'. The right is not absolute and only applies in certain circumstances.

You have the right to have your personal data erased if:

- the personal data is no longer necessary for the purpose which Hornbill originally collected or processed it for; or
- Hornbill are relying on consent as our lawful basis for holding the data, and then you withdraw your consent; or
- Hornbill are relying on legitimate interests as our basis for processing, you object to the processing of your data, and there is no overriding legitimate interest to continue this processing; or
- Hornbill are processing the personal data for direct marketing purposes and you object to that processing; or
- Hornbill have processed the personal data unlawfully (i.e. in breach of the lawfulness requirement of the 1st principle); or
- Hornbill have to erase the personal data to comply with a legal obligation.

Hornbill will tell other organisations about the erasure of personal data where:

- the personal data has been disclosed to others; or
- the personal data has been made public in an online environment (for example on social networks, forums or websites).

If Hornbill has disclosed the personal data to others, Hornbill will contact each recipient and inform them of the erasure, unless this proves impossible or involves disproportionate effort. If asked to by you, Hornbill will also inform you about these recipients.

Where personal data has been made public in an online environment Hornbill will take reasonable steps to inform other controllers who are processing the personal data to erase links to, copies or replication of that data. When deciding what steps are reasonable Hornbill will take into account available technology and the cost of implementation.

The right to erasure does not apply if processing is necessary for one of the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation;
- for the performance of a task carried out in the public interest or in the exercise of official authority;
- for archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or

- for the establishment, exercise or defence of legal claims.

The GDPR also specifies two circumstances where the right to erasure will not apply to special category data:

- if the processing is necessary for public health purposes in the public interest (e.g. protecting against serious cross-border threats to health, or ensuring high standards of quality and safety of health care and of medicinal products or medical devices); or
- if the processing is necessary for the purposes of preventative or occupational medicine (e.g. where the processing is necessary for the working capacity of an employee; for medical diagnosis; for the provision of health or social care; or for the management of health or social care systems or services). This only applies where the data is being processed by or under the responsibility of a professional subject to a legal obligation of professional secrecy (e.g. a health professional)

Hornbill may refuse to comply with a request for erasure if it is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature. If Hornbill considers that a request is manifestly unfounded or excessive we may:

- request a reasonable fee to deal with the request; or
- refuse to deal with the request.

In either case Hornbill will justify our decision to you.

Hornbill will base the reasonable fee on the administrative costs of complying with the request. If Hornbill decides to charge a fee we will contact you promptly and inform you. Hornbill will not comply with the request until we have received the fee.

If Hornbill refuses to comply with a request for erasure we will inform you without undue delay and within one month of receipt of the request. We will inform you about:

- the reasons Hornbill are not taking action; and
- your right to make a complaint to the ICO or another supervisory authority; and
- your ability to seek to enforce this right through a judicial remedy.

Hornbill will also provide this information if they request a reasonable fee or need additional information to identify you.

A request does not have to include the phrase 'request for erasure' or Article 17 of the GDPR, as long as one of the conditions listed above apply. This presents a challenge as any of Hornbill's employees could receive a valid verbal request. Hornbill have a legal responsibility to identify that you have made a request to Hornbill and handle it accordingly. Hornbill will consider which of your staff who regularly interact with individuals may need specific training to identify a request.

Hornbill will record details of the requests it receives, particularly those made by telephone or in person. Hornbill will check with the requester that it has understood their request, as this can help avoid later disputes about how Hornbill have interpreted the request. Hornbill will keep a log of verbal requests.

Hornbill will act upon the request without undue delay and at the latest within one month of receipt.

Hornbill may extend the time to respond by a further two months if the request is complex or Hornbill have received a number of requests from you. Hornbill will let you know without undue delay and within one month of receiving your request and explain why the extension is necessary.

If Hornbill has doubts about the identity of the person making the request Hornbill can ask you for more information. Hornbill will only request information that is necessary to confirm who you are. The key to this is proportionality. Hornbill will take into account what data it holds, the nature of the data, and what Hornbill is using it for.

Hornbill will let you know without undue delay and within one month that it needs more information from you to confirm your identity. Hornbill will comply with the request until it have received the additional information.

RIGHT TO RESTRICT PROCESSING

Article 18 of the GDPR gives you the right to restrict the processing of your personal data in certain circumstances. This means that you can limit the way that Hornbill uses your data. This is an alternative to requesting the erasure of your data.

You have the right to restrict the processing of your personal data where you have a particular reason for wanting the restriction. This may be because you have issues with the content of the information Hornbill holds or how Hornbill has processed your data. In most cases Hornbill will not restrict processing of your personal data indefinitely, but Hornbill will need to have the restriction in place for a certain period of time.

You have the right to request Hornbill restrict the processing of your personal data in the following circumstances:

- you contest the accuracy of your personal data and Hornbill are verifying the accuracy of the data; or
- the data has been unlawfully processed (i.e. in breach of the lawfulness requirement of the first principle of the GDPR) and you oppose erasure and requests restriction instead; or
- Hornbill no longer need the personal data but you need Hornbill to keep it in order to establish, exercise or defend a legal claim; or
- You have objected to you processing your data under Article 21(1), and Hornbill are considering whether its legitimate grounds override yours.

Hornbill will automatically restrict the processing whilst it is considering the personal data's accuracy or the legitimate grounds for processing the personal data in question.

Hornbill may use a number of different methods to restrict data, such as:

- temporarily moving the data to another processing system; or
- making the data unavailable to users; or
- temporarily removing published data from a website.

Hornbill will consider how it stores personal data that it no longer need to process but you have requested Hornbill restrict (effectively requesting that Hornbill does not erase the data).

Hornbill will use such technical measures as necessary to ensure that any further processing cannot take place and that the data cannot be changed whilst the restriction is in place. Hornbill will also note on our systems that the processing of this data has been restricted.

Hornbill will not process the restricted data in any way except to store it unless:

- Hornbill has your consent; or
- it is for the establishment, exercise or defence of legal claims; or
- it is for the protection of the rights of another person (natural or legal); or
- it is for reasons of important public interest.

If Hornbill have disclosed the personal data in question to others, Hornbill will contact each recipient and inform them of the restriction of the personal data - unless this proves impossible or involves disproportionate effort. If asked to by you, Hornbill also inform you about these recipients.

When the restriction is on the grounds that:

- you have disputed the accuracy of the personal data and Hornbill are investigating this; or
- you have objected to Hornbill processing your data on the basis that it is necessary for the performance of a task carried out in the public interest or the purposes of Hornbill's legitimate interests, and Hornbill are considering whether our legitimate grounds override yours.

Once Hornbill has made a decision on the accuracy of the data, or whether our legitimate grounds override yours, Hornbill may decide to lift the restriction. If Hornbill does this, Hornbill will inform you before it lifts the restriction.

If Hornbill are informing you that Hornbill are lifting the restriction (on the grounds that we are satisfied that the data is accurate, or that our legitimate grounds override yours) Hornbill will also inform you of the reasons for its refusal to act upon your rights under Articles 16 or 21. Hornbill will also inform you of your right to make a complaint to the ICO or another supervisory authority; and your ability to seek a judicial remedy.

Hornbill may refuse to comply with a request for restriction if the request is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature. If Hornbill consider that a request is manifestly unfounded or excessive it may:

- request a reasonable fee to deal with the request; or
- refuse to deal with the request.

In either case Hornbill will justify its decision to you.

Hornbill will base the reasonable fee on the administrative costs of complying with the request. If Hornbill decides to charge a fee Hornbill will contact you promptly and inform you. Hornbill will not comply with the request until Hornbill has received the fee.

If Hornbill refuses to comply with a request for restriction it will inform you without undue delay and within one month of receipt of the request. Hornbill will inform you about:

- the reasons Hornbill is not taking action; and
- your right to make a complaint to the ICO or another supervisory authority; and
- your ability to seek to enforce this right through a judicial remedy.

Hornbill will also provide this information if Hornbill requests a reasonable fee or need additional information to identify you.

A request does not have to include the phrase 'request for restriction' or Article 18 of the GDPR, as long as one of the conditions listed above apply.

This presents a challenge as any of our employees could receive a valid verbal request. Hornbill has a legal responsibility to identify that you have made a request to Hornbill and handle it accordingly. Hornbill will consider which of our staff who regularly interact with individuals may need specific training to identify a request.

Hornbill will record details of the requests it receives, particularly those made by telephone or in person. Hornbill will check with you that it has understood your request, as this can help avoid later disputes about how Hornbill have interpreted the request. Hornbill will keep a log of verbal requests.

Hornbill will act upon the request without undue delay and at the latest within one month of receipt.

Hornbill may extend the time to respond by a further two months if the request is complex or Hornbill have received a number of requests from you. Hornbill will let you know within one month of receiving your request and explain why the extension is necessary.

If Hornbill have doubts about the identity of the person making the request Hornbill may ask for more information. Hornbill will only request information that is necessary to confirm who you are. The key to this is proportionality. Hornbill will take into account what data it holds, the nature of the data, and what Hornbill are using it for.

Hornbill will let you know without undue delay and within one month that it needs more information from you to confirm your identity. Hornbill will not comply with the request until it has received the additional information.

RIGHT TO DATA PORTABILITY

The right to data portability allows you to obtain and reuse your personal data for your own purposes across different services. It is intended to allow you to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

The right to data portability only applies:

- to personal data you have provided us; and
- where the processing is based on your consent or for the performance of a contract; and
- when processing is carried out by automated means

Hornbill will provide the personal data in a structured, commonly used and machine readable form. Open formats include CSV files. Machine readable means that the information is structured so that software can extract specific elements of the data. This enables other organisations to use the data.

The information will be provided free of charge.

If you request it, Hornbill may be required to transmit the data directly to another organisation if this is technically feasible. Hornbill will not be required adopt or maintain processing systems that are technically compatible with other organisations.

If the personal data concerns more than one individual, Hornbill will consider whether providing the information would prejudice the rights of any other individual.

Hornbill will respond without undue delay, and within one month.

This can be extended by two months where the request is complex or Hornbill has received a number of requests from you. Hornbill will inform you within one month of the receipt of the request and explain why the extension is necessary.

Where Hornbill is not taking action in response to a request, Hornbill will explain why to you, informing you of your right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

RIGHT TO OBJECT

You have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling); and

- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

If you raise an objection to the processing of your personal data by Hornbill then Hornbill will stop processing the data unless:

- Hornbill can demonstrate compelling legitimate grounds for the processing, which override your interests, rights and freedoms; or
- the processing is for the establishment, exercise or defence of legal claims.

Hornbill will inform you of your right to object at the point of first communication. This will be explicitly brought to your attention and will be presented clearly and separately from any other information.

Hornbill will stop processing personal data for direct marketing purposes as soon as it receives an objection. There are no exemptions or grounds to refuse.

Hornbill will deal with an objection to processing for direct marketing at any time and free of charge.

RIGHTS RELATED TO AUTOMATED DECISION MAKING AND PROFILING

Hornbill does not carry out any automated decision making or profiling.

PROTECTIVE MEASURES

The Board of Directors and senior management of Hornbill are committed to preserving the confidentiality, integrity and availability of personal data processed by the company. To that end Hornbill takes the following protective measures:

1. Personal data is only accessible to those authorised to access it and all employees, sub-contractors, project consultants and any other external parties are made aware of their responsibilities to preserve information security, to report security breaches, and to act in accordance with security policies whilst doing so. The consequences of security policy violations are described in Hornbill's disciplinary processes contained within the HR policy. All staff receive information security awareness training and specialist employees will receive appropriately focused training as required to meet Hornbill's business, contractual, and regulatory requirements and obligations.
2. Hornbill is committed to compliance with all national and, where appropriate, international laws relating to the protection of personal data and individual privacy (including GDPR); this policy applies to all personal data processed by Hornbill. Hornbill continuously reviews and audits operations and security arrangements to ensure personal data is processed appropriately by authorised Hornbill personnel.
3. Hornbill maintains rigorous policies in respect to mobile security and requires mobile devices (laptops, mobile computers, PDAs, mobile phones, USB sticks and other similar memory devices) to have: (i) password protection, (ii) where appropriate/possible to be encrypted, (iii) the most recent operating system and application security-related patches, fixes and updates to be installed. Hornbill also requires notebook computers to be physically protected against theft and damage while in transit, in storage or in use and that, in cases of loss or theft this is reported immediately. Furthermore, Hornbill ensures users are appropriately trained, understand and can carry out their agreed security obligations.
4. Hornbill undertakes vetting of all Hornbill personnel in line with BS7858:2012
5. Hornbill personnel, with access to personal data, are provided with and sign a contract of employment which includes a confidentiality agreement covering the various responsibilities and actions required of signatories to avoid unauthorized information disclosure, the permitted use of the information, the signatories' rights in respect of that information and the required actions on termination of the agreement.

6. Hornbill will monitor for, analyse and respond to information security incidents immediately they are seen or experienced and report all such incidents to the Information Security Manager who will be responsible for undertaking an assessment and categorising the reported incident in a timely manner and in accordance with Hornbill's documented operating procedures.
7. Hornbill will report to you any; access to, alteration, disclosure of, accidental or unlawful destruction, or loss to your personal data (a "Breach"). An initial report will be made to you. As Hornbill investigates or otherwise becomes aware of further information, and unless restricted by any applicable law, Hornbill will provide all further information pertaining to the nature and impact of the Breach.

SCHEDULE 1

HORNBILL EMPLOYEES AND EX EMPLOYEES

What is the purpose for which the data has been collected?

Hornbill holds your personal data to enable it to:

1. Manage its payroll responsibilities to you and HMRC
2. To monitor your training and development
3. To monitor your absences and vacations
4. To comply with its pension obligations
5. To record any conduct or disciplinary related matters
6. To record any grievances or whistle blowing matters
7. To comply with its other legal obligations as an employer, including but not limited to:
 - a. Equal opportunities legislation
 - b. Health and safety legislation
 - c. Paternity and maternity legislation
 - d. Adoption legislation
 - e. Flexible working legislation
 - f. The European Working Time Directive
 - g. The General Data Protection Regulation and Data Protection Act 2018
8. Record knowledge – for example track who wrote a particular piece of code or who posted a particular post in Hornbill

What is the lawful basis on which we process the data?

The lawful basis for holding personal data depends upon the nature of the data and details are given in the next section.

What categories of data are obtained and how do we ensure that only data that is needed for the purpose is collected?

Data Class	Lawful Basis	Special Category
Name	Contractual and Legal	
Home Address	Contractual and Legal	
Telephone Numbers	Contractual and Legal	
Bank Account	Contractual	
Emergency Contact	Legal	
Medical Details (1)	Legal	Data concerning health
P45 from former employer	Contractual and Legal	
Tax Codes from HMRC	Contractual and Legal	
Death in Service Beneficiary Details	Contractual	
Payroll Information (2)	Contractual and Legal	
Exit Questionnaire	Contractual	
Offer Letter	Contractual	
Salary Review Letters	Contractual	
Disciplinary Records	Contractual	
Holiday Records	Contractual and Legal	
Sickness Records	Contractual and Legal	Data concerning health
Driver's License (3)	Legal	
Car Insurance	Legal	
Car MOT and Service Records	Legal	
Criminal Convictions	Contractual	Criminal convictions and offences

Bankruptcy Proceedings	Contractual	Criminal convictions and offences
Redundancy or Termination Records	Contractual and Legal	
Letter of Resignation	Contractual	
Health and Safety Records (4)	Contractual and Legal	
Maternity/Paternity/Adoption Records	Contractual and Legal	
Commission or Bonus Plan	Contractual	
References from Former Employers	Contractual	
References for Future Employers	Contractual	
Background checks (5)	Contractual	
Proof of Right to Work in UK	Legal	

- (1) Relevant to your work at Hornbill or which may need treatment whilst you are working for Hornbill (including but not limited to allergies, epilepsy, heart conditions, diabetes, back problems, sight problems etc.)
- (2) Including but not limited to salary, overtime, commission, bonus, pension contributions, private medical, educational loans, company advances, cycle to work scheme etc.
- (3) endorsements to or loss of driver's licence if a car is used for work
- (4) Including but not limited to workstation assessment records (contractual and legal)
- (5) Before and during employment

When a contract is terminated by way of resignation, redundancy or dismissal and the contract does not contain provision for the retention of personal data for up to 7 years after the employment is terminated then Hornbill will continue to retain that personal data on the basis of its Legitimate Interests.

Who are the recipients of the data?

Hornbill will only share personal data with third parties where there is a legal or contractual requirement to do so. Hornbill will only share such data as is the minimum required for that third party to deliver on their contractual obligations.

The organisations we currently share the data with are as follows:

- HM Revenue and Customs
- Vitality (private medical provider)
- Centor (our insurance and benefits broker)
- BUPA (our travel insurance provider)
- Unum (our death in service provider)
- Iris (our payroll services provider)
- NSSA (our security screening services provider)
- Reference requests from future employers and others (e.g. potential landlords, mortgage companies). Note that we will only provide this data if we have explicit written approval from you to do so
- Security screening related data to customers or potential customers. Note we will only provide this data if we have explicit written permission from you to do so.

Information held on each employee will only be provided internally to the employee's Line Manager and Senior Management or Directors and those involved with payroll activities. The information so provided will be only that information that they require to carry out processing for their particular lawful purpose.

Which countries will we transfer the data to?

Hornbill does not transfer the data outside the EEA and the country in which you are based.

Where did we get the data from?

The data will be provided to us by you and by the recipient organisations listed above

How do we ensure that the data is kept accurate and up to date?

Whilst you are employed by Hornbill we expect you to update us if any of the personal data listed above changes. If we receive updated personal data from any of the organisations listed above we update our records as soon as practicable.

When you leave Hornbill, we will rely on you to update us if your personal data changes, particularly in respect of your contact details.

How do we ensure that inaccuracies are corrected?

The nature of the data is such that it is used in our daily interactions with you so if there are any inaccuracies if they are not corrected they will quickly be picked up and dealt with.

How do we ensure that data that is no longer required for the purpose for which it is collected is deleted?

Hornbill will keep personal data on file for approximately 6 years from the date an employee leaves the company.

On or shortly after the 31st March each year the Human Resources files will be reviewed and any files that are over 6 years old, providing there are no ongoing legal matters in relation to the file, will be securely destroyed using shredding in the case of paper records and appropriate permanent destruction in the case of electronic or other records. Each time a file is destroyed a note of its destruction will be made in a register. The electronic systems in which we record personal data are as follows:

1. Human Resources data and copies of documents are stored in NetSuite. The user record and all attached files will be permanently deleted.
2. The Iris payroll system. The user record will be permanently deleted.
3. Holiday and other absence data is recorded in Hornbill. This data will be permanently deleted.
4. Cloud storage of security screening data by NSSA, our security screening contractor.

The timing of the annual review means that if your leaving date is on the 1st April we will destroy your files around 7 years after you leave Hornbill.

Backups that contain personal data will be deleted shortly after the deletion of the data to ensure it cannot be restored.

Hornbill will retain records of applicants for vacant positions for 6 months, after which they will be destroyed.

For avoidance of doubt once your files are destroyed Hornbill will have no personal data other than a record of your surname, initial, leaving date and date of destruction/deletion of your file. After the data is destroyed we will no longer be able to respond to any reference requests.

You may have recorded personal data in the Hornbill system or other storage places on the Hornbill network. It is incumbent on you to ensure that this personal data is deleted before you leave the company. Transactional postings in Hornbill are not deleted and you should ensure you do not record personal data in the timelines unless you irrevocably agree that it will remain there after you have left Hornbill.

How do we ensure that the data is secure?

Hornbill takes the generic Protective Measures set out above to ensure data is kept secure. Furthermore, the following specific Protective Measures are taken in respect of HR data:

- Paper records are kept in a secure cabinet and access is controlled by the CFO. Paper records will normally be historic documents as Hornbill now scans all paperwork and files it electronically.
- Electronic records are stored in four locations
 1. In our Iris payroll system which is kept on a secure server and has password access which is restricted to the CFO and any employees responsible for processing the payroll.
 2. On our NetSuite system in a secure folder. Access to the secure folder is restricted to the CFO and any employees responsible for processing the payroll.
 3. In Hornbill access to the holiday and sickness records is restricted to the individuals' manager and that managers manager, etc. The CFO also has access to the data.
 4. NSSA provide a cloud storage facility for the security screening data and reports. Only the CFO has access to this data.