Employee Privacy Policy

Version 2.3 Feb 2024

Version Control

Revision Date	Version	Summary of Changes	Author
June 2020	0.1	Document Creation	
June 2020	1.0	Minor updates and amendments following review	
17/12/21	2.0	Full review	Suzanne Evans – Compliance Manager
08/03/22	2.1	Final review and incorporate KD comments	Suzanne Jones – Compliance Manager
17/02/23	2.2	Annual review, updated to cover current processes and suppliers	Suzanne Jones – Compliance Manager

Document Classification

Classification	Examples	Reason for Classification
Private	Any generic documents shared with all staff and third parties, i.e. compliance policies	This document is shared with all Vypr staff and contractors

Approvers

Name	Role	Date
Kate Downing	People Manager	30/04/24
Tasmin Sibbald	Operations Director	30/04/24

Document Review

This policy will be reviewed at least annually by the Compliance Manager and People Manager.

Contents

Vypr Employee Privacy Policy

In this Privacy Policy the terms, 'we' or 'us' is Vypr.

Your privacy is important to us, and we are committed to keeping your information secure and managing it in accordance with our legal responsibilities under data protection legislation. We are registered with the Information Commissioner's Office (ICO) as a data controller under registration number ZA026869.

An important part of managing this, is to ensure that no one has access to any business or personal information that you shouldn't. If this does happen, you must ensure you notify the Data Protection Officer immediately.

This Privacy Policy details the personal information we collect from you and process through your employment with us, what we use your information for, who we share your information with, how we protect your information, how long we keep it for, our responsibilities and your rights.

1 – Personal Information We Process

We process your personal information which:

- You give us when you apply for a job directly with us
- We obtain from a recruitment agency when they supply us with an application from you
- We receive from any third-party companies we use to assess your technical abilities
- We receive from third parties such as credit reference agencies, criminal record and fraud prevention agencies, pension providers, insurance providers, former employers, academic and professional qualifications, psychometric testing, etc
- We collect during your employment relating to your performance, development, and training

This personal information includes your name, address (including address history), telephone number, email address, date of birth, National Insurance number, employment history, references, official documentation (i.e. passport, driving licence, birth certificate), bank details, credit history, information regarding your emergency contacts, qualifications, training and competency records, identifiers assigned to your computer or other internet connected device including your IP addresses, information linked to your mobile telephone number.

With your consent, we will also collect special categories of personal data including health information regarding a disability, illness or impairment, ethnicity or criminal

offence data. See Section 4 on Special Categories of Personal Data below for further details.

Our websites and some third-party websites use cookies (including Google Analytics) to monitor users' activities, including downloads and pages viewed. Certain websites are blocked, and we restrict how much time a user can spend on a website which is not linked to business activities. We may conduct checks on your browser history at any time.

2 - Use of Your Information

Your information will be used by us for the following reasons:

PURPOSE OF PROCESSING	LEGAL BASIS FOR PROCESSING
During Employment	
To process payroll and pay out of pocket expenses, a record is kept of employees' bank details, National Insurance numbers and taxation records	• Contract
To help you manage any health conditions and to record if you have a Disability on Employment Hero, to ensure we are offering the correct level of support required	• Contract
To manage absence, both planned and unplanned and validate fitness and ability to return to work	• Contract
For training purposes and to enhance or review performance	• Contract
To provide hotel accommodation, company or hire cars	• Legitimate interests

To maintain governance records, including mandatory training, conflicts of interest register, gifts and hospitality log.	• Legal obligation
Security and crime prevention including CCTV	
To monitor access to the office and restricted areas, and to monitor your use of IT systems and applications to ensure it meets acceptable use requirements	• Contract • Legal obligation
Complying with Legal Obligations	
To prevent, investigate and prosecute crime, fraud, and money laundering	• Legal obligation
For auditing purposes	• Legal obligation
If we are obliged to disclose information for legal reasons	• Legal obligation
Other	
To transfer information to any entity which may acquire rights in us	• Contract
For any other purpose to which you agree	• Consent

Where we or third parties (see below) process your personal information, it will be processed:

- Because we or they need to do so as a direct consequence of fulfilling a request (for example, to check your identity to consider you for a job); or
- To comply with legislation, or as permitted by legislation; or

- On the basis that we or they have a legitimate interest (for example, managing our risk or preventing crime, fraud, and money laundering), and to protect our business.

3 – Who We Share Your Information With

Third parties including Employment Hero (HR), UCheck (HR), Fairstone (HR), EE (HR), Everything Tech (IT Support), NJC Business Solutions (Payroll), J Coleman (Business Support), Saville (Psychometric Testing), Perkbox (flexible benefits), Core Learning (E-Learning Platform), Medicash, HMRC, Equifax, DBS, Reference requests, Insurance Companies, Xero and The People's Partnership (previously known as The People's Pension), with whom we may need to share personal information to help us manage your employment with us. It also includes Regulators or government bodies to comply with any legal obligations. These companies:

- Need to know the information to provide us or you with a service (including flexible benefits providers)
- Process information on our behalf to help run some of our internal business operations including background checks, surveys and assessments, training, email distribution, storage of documentation
- Check your identity and obtain credit references
- Assist us to better manage, support or develop our employees and comply with our legal and regulatory obligations

These parties may be in the UK, or other countries in the European Economic Area (EEA) or elsewhere in the world. Whenever we or service providers transfer and/or process your personal information outside of the EEA, we will ensure they impose the standard contractual obligations on the recipients of that information to protect your personal information to the standard required in the UK.

4 - How we Protect your Information

We invest in technological resources to protect your personal information, from loss, misuse, unauthorised access, modification or disclosure and we have put additional measures in place, such as limiting those people who have access to your data. Further information on this can be provided by contacting the Data Protection Officer.

Emails sent via the internet can be subject to interception, loss, or possible alteration, therefore we cannot guarantee their security. Although we will do our best to protect your personal information, we cannot guarantee the security of your data sent by email and therefore will have no liability to you for any damages or other costs in relation to emails sent by you to us via the internet.

Special categories of Personal Data

This includes sensitive personal data, such as biometric and genetic information that can be processed to identify a person. Other categories include race, ethnicity, political views, religion, health, sex life and orientation.
We do not generally process such information, unless you have voluntarily provided the information to us (where we have asked for your specific consent), or we are required to do so, for example, where you have notified us of a medical issue to allow for reasonable adjustments to be made. This information is held by the People Manager and is only shared with other members of staff with your consent, i.e. Health and Safety Officer, Line Manager.
The UK GDPR gives extra protection to "personal data relating to criminal convictions and offences or related security measures". We refer to this as criminal offence data. This covers a wide range of information about:

- criminal activity;
- allegations;
- investigations; and
- proceedings.

Processing criminal offence data is allowed for employment reasons. You have a duty to make the People Manager aware if you face any allegations or investigations involving criminal activity. This information will be treated in the strictest confidence and only shared with a limited number of people, i.e. your Line Manager and Compliance Manager.

5 – Vypr's Responsibilities as a Data Controller

All data Vypr processes must comply with the 7 key data protection principles:

a) Lawfulness, fairness and transparency – this requires Vypr to identify the valid grounds for collecting and using personal data, to only use personal data in a way which is fair and to be clear, open and honest about how we use personal data.

b) Purpose limitation – this requires Vypr to be clear about our purposes for processing your data from the start and share this information with you.
c) Data minimisation – this requires Vypr to ensure the personal data we process is sufficient to properly fulfil the stated purpose, is relevant to that purpose and is limited to what is necessary.
d) Accuracy – this requires Vypr to ensure all personal data is accurate and kept up to date.
e) Storage limitation – this requires Vypr to not keep personal data for longer than we need to.

Below is a table detailing how long we keep employee data for:

Type of personal information	**Retention period**
Recruitment personal data including CVs, Application forms, assessments, tests and results, Reference and Employment Checks, Identity and Financial Information and Documents, Employee offer letters and Contracts	Unsuccessful applicants for 6 months from interview, and a further 6 months if we have your permission Successful applicants 6 years after the end of employment.
Normal personal data, including employee benefits, tax and salary details, pension and retirement records, appraisals (and other documentation regarding hiring, promotion, demotion, transfer, lay-off, termination or selection for training)	6 years after the end of employment
Special categories of personal data: data regarding health, including sickness and absence records, injury and accident incident reports, working from home risk assessments, health and safety risk assessments	6 years after the end of employment
Supplemental record for each occupational injury or illness (OSHA Form 101); Log and Summary of Occupational Injuries and Illnesses (OSHA Form 200)	6 years after the end of employment
Records of Disciplinary Actions	These come off the record after the duration of the warning has expired
Employees bank details	3 months after employment has ended
Personal location	Attendance records for training 6 years after the end of employment

	Corporate card statements are retained for 6 years, these may identify location of employees
Call Recordings (with prospective/actual customers)	12 months from date of call

f) Integrity and confidentiality (security) – this requires Vypr to have appropriate security measures in place to protect the personal data we hold.

g) Accountability – this requires Vypr to take responsibility for what we do with personal data and how we comply with the other principles above. We must have appropriate measures and records in place to demonstrate our compliance.

6 – Your Rights

Data Protection legislation provides individuals with the following rights:

a) The right to be informed – this is about providing individuals with clear and concise information about what you do with their personal data. This Privacy Policy is how Vypr comply with this requirement.

b) The right of access – this is about individuals having the right to obtain a copy of any personal data Vypr hold on them (also known as subject access). This only applies to an individual's own personal data and not to information relating to other people (unless the information is also about them). The request can be made verbally or in writing, and Vypr has one month to respond and provide the information. If we have doubts about the identity of the person making the request (i.e. an ex-employee), we can ask for information to confirm their identity, and the one-month response time does not start until we receive this.

c) The right to rectification – this is about individual's having the right to have inaccurate personal data rectified. Inaccurate data is defined as "incorrect or misleading as to any matter of fact".

d) The right to erasure – this is about individual's having the right to have personal data erased, also known as the "right to be forgotten". This right is not absolute and only applies in certain circumstances. For the processing of data as an employee of Vypr, the right to erasure will not apply as we are legally obliged to keep a copy of your personal information for the periods documented above.

e) The right to restrict processing – this gives individuals the right to restrict the processing of their personal data in certain circumstances. This may be where they have a reason for wanting the restriction due to issues with the content of

information we hold or how we have processed their data. All requests will be considered on an individual basis.

f) The right to data portability – this gives individuals the right to receive personal data they have provided to a controller in a structured, commonly used, and machine-readable format. It also gives them the right to request a controller transmits this data directly to another controller. This right only applies where the lawful basis for processing this information is with your consent or for the performance of a contract.

g) The right to object – this gives individuals the right to object to the processing of their personal data at any time, but only in certain circumstances.

h) Rights in relation to automated decision making and profiling – Vypr do not process any employee personal data for these reasons.

Contact
For further information or to exercise any of your rights, please contact:
Data Protection Officer and Compliance Manager - Suzanne Jones
People Manager – Kate Downing

Complaints Process
If you have a complaint about how we have handled your personal information, please contact us using the details above and we will investigate your complaint. You also have the right to complain to the Information Commissioner's Office – www.ico.org.uk but you should contact us in the first instance.

We will review this Privacy Policy at least annually and make further updates from time to time. Any changes to this Policy will be notified by us to you and you will be asked to read and confirm that you have done so.