

# **Employee Consent and Privacy Policy**



## **Optindigo Instructions**

#### What does this document do?

This document provides templates for employee consent forms and privacy policies.

## Do I need to complete this document?

You need to review this document if you have full-time or part-time employees, contractors, volunteers, or other people working in your organisation.

## Where can I get more help?

You can call, email or chat to us about Optindigo during office hours. For more helpful advice or guidance check out our Optindigo useful links page.

## How often do I need to update this document?

You should review this document every 3 months to ensure you meet the GDPR and these terms meet your business requirements.



## Introduction

The GDPR specifies regulations on how you manage your data. This of course includes data about your employees, volunteers, contractors and other staff. This data often includes personal information and in some cases sensitive data such as religion, medical information, family details and financial information. As such, it is vital that this information is handled carefully and in line with the GDPR regulations.

This document includes templates for an employee consent form plus privacy policy. You can use these documents as the basis of your companies' employment documents.



## **Example Privacy Notice**

## How your information will be used

Cheshire Companions take the privacy and security of your personal data very seriously.

- 1. As your employer, the Company needs to keep and process information about you for normal employment purposes. We may update this notice at any time and we may provide you with an additional privacy notice from time to time. The information we hold and process will be used for our management and administrative use only. We will store and use it to enable us to run the business and manage our relationship with you effectively, lawfully and appropriately, during the recruitment process, whilst you are working for us, at the time when your employment ends and after you have left. This includes using information to enable us to comply with the employment contract, to comply with any legal requirements, pursue the legitimate interests of the Company and protect our legal position in the event of legal proceedings. If you do not provide this data, we may be unable in some circumstances to comply with our obligations and we will tell you about the implications of that decision. In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you.
- 2. Once you are no longer an employee, worker or contractor of the company we will retain and securely destroy your personal information in accordance with applicable laws and regulations.
- 3. As a company pursuing Escort Agency activities, we may sometimes need to process your data to pursue our legitimate business interests, for example to prevent fraud, for administrative purposes or reporting potential crimes. The nature of our legitimate interests are *INSERT NATURE OF LEGITIMATE INTERESTS*. We will never willingly process your data where these interests are overridden by your own interests. We aim to process your personal data lawfully, fairly and in a transparent way.
  - To collect your personal data only for valid purposes that we have advised you about and to
    not use your personal data in any way that is incompatible with those purposes (unless we
    have notified you and explained the lawful ground that allows us to do so)
  - To only process your personal data to the extent necessary for the purposes we have advised you about
  - To keep your personal data accurate and kept up to date
  - To keep your personal data only as long as necessary for the purposes we have told you about
  - To keep your personal data secure
  - Most of the information we hold will have been provided by you. However, some may come from other internal sources, such as your manager, or in some cases, external sources, such as referees



We will collect, store, and use the following categories of personal data about you:

- Personal contact details such as name, title, date of birth, gender, addresses, telephone numbers and personal email addresses
- Marital status and dependents
- Next of kin and emergency contact information
- Bank account details, payroll records and tax status information
- Salary, annual leave, pension and benefits information, national insurance number
- Location of employment or workplace and start date
- Copy of driving license/passport
- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process)
- Employment records (including job titles, work history, working hours, training records and professional memberships)
- Details of your existing and previous salary
- Performance information and disciplinary and grievance information
- CCTV footage and other information obtained through electronic means such as electronic key card records
- Information about your use of our information and communications systems
- Photographs/ID passes

#### PURPOSES FOR WHICH WE PROCESS YOUR PERSONAL DATA

We will process your personal data for the following purposes:

- Making a decision about your recruitment or appointment
- Payroll and deducting employee's National Insurance and tax
- Providing certain benefits to you
- Liaising with your pension provider
- Administering your contract
- Business management and planning, including accounting and auditing
- Conducting performance reviews, managing performance and determining performance requirements
- Making decisions about salary reviews and compensation
- Assessing qualifications for a particular job or task, including decisions about promotions



- Gathering evidence for possible grievance or disciplinary hearings
- Making decisions about your continued employment or engagement
- Making arrangements for the termination of our working relationship
- Education, training and development requirements
- Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work
- Ascertaining your fitness to work
- Managing sickness absence
- Complying with health and safety obligations
- Preventing fraud
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution
- To conduct data analytics studies to review and better understand employee retention and attrition rates
- Equal opportunities monitoring
- 4. The sort of information we hold includes your application form and references, your contract of employment and any amendments to it; correspondence with or about you, for example letters to you about a pay rise or, at your request, a letter to your mortgage company confirming your salary, information needed for payroll, benefits and expenses purposes, contact and emergency contact details, records of holiday, sickness and other absence, information needed for equal opportunities monitoring policy and records relating to your career history, such as training records, appraisals, other performance measures and where appropriate, disciplinary and grievance records *INSERT ANY FURTHER CATEGORIES HERE*.
- 5. Inevitably, you will, of course be referred to in many company documents and records that are produced by you and your colleagues in the course of carrying out your duties and the business of the company.
- 6. Where necessary, we may keep information relating to your health that could include reasons for absence and GP reports and notes. This information will be used in order to comply with our company health and safety and occupational health obligations to consider how your health affects your ability to do your job and whether any adjustments to your job might be appropriate. We will also need this data to administer and manage statutory and company sick pay, *ADD BENEFITS e.g. health insurance or life insurance policies*.
- 7. Where we process special categories of information relating to your racial or ethnic origin, political opinions, religious and philosophical beliefs, trade union membership, biometric data or sexual orientation, we will always obtain your explicit consent to those activities unless this is not required by



law or the information is required to protect your health in an emergency. Where we are processing data based on your consent, you have the right to withdraw that consent at any time.

- 8. In addition, we monitor computer (and telephone/mobile telephone) use, as detailed in our computer/telephone/electronic communications/expenses policy, available (in the company handbook/on the intranet). We also keep records of your hours of work by way of our clocking on and off system, as detailed in the company handbook/intranet.
- 9. Other than as mentioned below, we will only disclose information about you to third parties if we are legally obliged to do so or where we need to comply with our contractual duties to you, for instance we may need to pass on certain information to [external payroll provider], pension or health insurance schemes.
- 10. We may transfer information about you to other group companies for purposes connected with your employment or the management of the company's business.
- 11. In limited and necessary circumstances, your information may be transferred outside of the EEA or to an international organisation to comply with our legal or contractual requirements. We have in place safeguards including *LIST OF SAFEGUARDS* to ensure the security of your data. A copy of the safeguards can be obtained from *INSERT HERE*.
- 12. We do use automated decision making (including profiling) in limited circumstances including to INSERT DETAILS. INCLUDE INFORMATION ABOUT THE LOGIC INVOLVED, THE SIGNIFICANCE AND ENVISAGED CONSEQUENCES OF THAT PROCESSING.
- 13. Your personal data will be stored for a period of *INSERT PERIOD HERE* or the criteria used for determining how long your data will be stored for is *INSERT CRITERIA HERE*.
- 14. If in the future we intend to process your personal data for a purpose other than that which it was collected for, we will provide you with information on that purpose and any other relevant information.

### **Your Rights**

Under the General Data Protection Regulation (GDPR) and The Data Protection Act 2018 (DPA) you have a number of rights with regard to your personal data

- Request access to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it
- Request correction of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected
- Request erasure of your personal information. This enables you to ask us to delete or remove
  personal information where there is no good reason for us continuing to process it. You also
  have the right to ask us to delete or remove your personal information where you have



exercised your right to object to processing (see below)

- Object to processing of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation that makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes
- Request the restriction of processing of your personal information. This enables you to ask us
  to suspend the processing of personal information about you, for example if you want us to
  establish its accuracy or the reason for processing it
- Request the transfer of your personal information to another party

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact Wesley Stafford in writing.

You will not have to pay a fee to access your personal data or to exercise any of the other rights under data protection laws. However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

15. You have the right to lodge a complaint with the Information Commissioner's Office if you believe that we have not complied with the requirements of the GDPR or DPA with regard to your personal data.

#### Identity and contact details of controller and data protection officer

Cheshire Companions is the controller (and processor) of data for the purposes of the DPA and GDPR.

If you have any concerns as to how your data is processed you can contact:

Wesley Stafford Data Protection Offer at info@cheshirecompanions.com

Insert details of any other relevant contacts

Эr y	/ou	can v	vrite	to t	hese	individ	luals	using	the	e ado	dress	ot	3 (	Grove	Par	k R	d, V	<b>Vrex</b> l	nam	LL1:	L 1I	ŊΥ
------	-----	-------	-------	------	------	---------	-------	-------	-----	-------	-------	----	-----	-------	-----	-----	------	---------------	-----	------	------	----

Signed	Date	



# **GDPR Checklist For Employers**

Take a look at this checklist to confirm that you have reviewed your contracts and associated documentation to include the appropriate privacy notice and consent forms.

Action	Comments	Completed?
EMPLOYEE INFORMATION		
AUDIT		
Identify what personal data		
you hold about employees		
and candidates (and where it		
came from)		
Identify all the ways in which		
you process personal data		
and the purposes of the		
processing		
Verify how long you		
currently retain the personal		
data and how long you need		
to keep the personal data for		
the purpose for which it is		
collected		
Identify any parties to whom		
you transfer personal data,		
including any international		
data transfers, for example,		
payroll and benefits		
providers and other group		
entities		
Review any associated		
contracts		
Identify any automated		
decision-making within HR		
processes, for example, in		
recruitment (automated		
rejection and short-listing),		
triggers for sickness absence		
or disciplinary action, attendance bonuses, shift		
and holiday roster, and		
employee monitoring		
Ensure the audit is properly		
documented		
Identify lawful basis for		
-iuenthy lawrul Dasis IUI		

optindigo THE GDPR

processing employee personal data under current data protection laws	
This will likely be employee	
consent, possibly obtained	
via a clause in the	
employment contract [NOTE:	
it is UNLIKELY to be consent	
under GDPR]	
Confirm current basis for	
processing "sensitive	
personal data" (including	
details of criminal	
convictions and offences)	
Identify lawful basis for	 
processing employee	
personal data under GDPR	
One of the following must	
apply:	
The employee gives valid	
consent (NOTE that for most	
purposes consent will not be	
deemed freely given due to	
the imbalance of power in	
the employer/employee	
relationship but it might be	
appropriate for things like	
surveys)	
Necessary to carry out the	
employment contract (eg	
taking financial data so you	
can pay them inc special	
leave/benefits)	
Necessary for the employer	
to comply with a legal	
obligation (eg taking social	
security data so that you can	
pay employer taxes, TU fees)	
Necessary to protect the	
vital interests of the	
employee or another person	
(eg to protect	
physical/mental	
health/disability status. To	
monitor sickness	
-absences/fitness for work	



Necessary in the public	
interest or if the employer is	
exercising official authority	
Necessary for a legitimate	
interest of the employer or a	
third party which is not	
overridden by the interests	
or fundamental rights and	
freedoms of the employee	
Identify lawful basis for	
processing special	
categories of employee	
personal data (sensitive	
data) under GDPR	
One of the following must	
apply:	
Valid explicit employee	
Necessary for comming out	
Necessary for carrying out	
employment rights and	
obligations, it is authorised	
by domestic or EU law and	
the employer has an	
appropriate policy document	
in place	
Necessary to protect the vital interests of the	
employee or another person	
where the employee is incapable of giving consent	
Processing by a foundation,	
association or not-for-profit	
with a political,	
philosophical, religious or	
trade union aim	
If the employee has made	
the personal data public	
Necessary for the employer	
to establish or defend legal	
claims	
Necessary for reasons of	
substantial public interest	
(including the processing of	
personal data revealing race,	
religious beliefs, health or	
sexual orientation for the	
<u>-                                      </u>	



purposes of promoting		
equality of treatment, and		
including processing		
necessary to determine		
eligibility for or benefits		
payable under an		
occupational pension		
scheme which can		
reasonably be carried out		
without the employee's		
consent), and the employer		
has an appropriate policy		
document in place		
Necessary for the		
assessment of the		
employee's working capacity		
either on the basis of		
domestic or EU law or		
pursuant to a contract with a		
health professional, and		
subject to confidentiality		
safeguards		
Identify lawful basis for		
processing of employee		
personal data relating to		
criminal convictions and		
offences under GDPR		
The processing must be		
authorised by domestic or		
EU law and, if authorised by		
domestic law, one of the		
following must apply:		
Necessary for carrying out		
employment rights and		
obligations and the employer		
has an appropriate policy		
document in place		
Valid employee consent		
(although consent will not be		
valid where there is a clear		
imbalance between the data		
subject and data controller,		
such as in an employment		
context)		
Necessary to protect the		
vital interests of the		
employee or another person Po	licy 12	indigo

where the employee is	
incapable of giving consent	
Processing by a foundation,	
association or not-for-profit	
with a political,	
philosophical, religious or	
trade union aim	
If the employee has made	
the personal data public	
Necessary for the employer	
to establish or defend legal	
claims	
DATA CLEANSING	<u>,                                    </u>
Update data retention policy	
based on results of audit and	
apply it (see the data	
retention policy in the pack)	
Securely delete or	
de-personalise all employee	
personal data where there is	
no lawful basis for the	
processing under GDPR	
Amend HR policies and	
processes	
For example, procedures	
relating to recruitment,	
promotions, compensation,	
disciplinary, grievances,	
performance management,	
sickness absence, employee	
monitoring and references,	
Conduct a data protection	
impact assessment (DPIA) if	
required	
Notify employees of changes	
to policies/handbook	
Automated decision-making	
(including profiling)	
Identify the lawful basis	
allowing you to take	
decisions that significantly	
affect an employee based on	
automated processing:	
Necessary to carry out the	
employment contract	
The employer notifies the	

Optindigo THE GDPR COMPANY

employee in writing of a	
decision based on	
automated processing and	
allows the employee the	
right to request a	
reconsideration within 21	
days	
Valid explicit employee	
consent	
Ensure that suitable	
measures to safeguard the	
employee's rights and	
freedoms and legitimate	
interests are in place,	
including the right to obtain	
human intervention, the	
right to express the	
employee's point of view	
and the right to appeal any	
automated decision	
Automated decision-making	
on the basis of special	
categories of personal data	
must be permitted by valid,	
explicit employee consent or	
in the substantial public	
interest, with suitable	
measures to safeguard the	
employee's rights and	
freedoms and legitimate	
interests	
Data transfers to third	
parties (other group entities	
and service providers)	
Identify lawful basis for all	
data transfers, including in	
particular any cross-border	
data transfers	
Put processor agreements in	
place where necessary	
Update procedures so that	
GDPR compliance forms part	
of due diligence when	
entering into a new contract	
with an HR supplier	
-Notify employees of the	



processing of personal data	
Draft new privacy notice for	
employees (use employee	
privacy notice not the	
website privacy notice)	
Ensure that procedures are	
updated so that the privacy	
notice is provided to	
employees and candidates	
when required as future	
personal data is collected or	
when the purpose of	
processing changes	
Data subject rights	
Update SAR policy and	
procedures: new timeline,	
free of charge unless request	
is manifestly unfounded or	
excessive, new information	
requirements	
Arrange updated training for	
all staff who handle SARs	
Establish procedures for	
dealing with the exercise of	
employee rights	
Data protection officer	
(DPO)	
Establish whether you are	
required to appoint a DPO	
If so, appoint a DPO, scope	
the role in accordance with	
GDPR requirements and	
provide them with the	
necessary training and	
resources	
If a DPO is not mandatory,	
consider designating a senior individual as having	
responsibility for data	
protection	
Training and review	
Arrange updated training for	
all staff who handle personal	
data	
uata	



Ensure that all arrangements	
and privacy notice are	
subject to regular review for	
continued compliance	
Ensure any policy document	
relating to the processing of	
special categories of	
personal data or criminal	
convictions is subject to	
regular review and updated	
where appropriate	

## **Consent Statement Example**

As part of your relationship with this company we will collect, store, and process details about you, your next of kin, your employment history, medical condition, and other information as described in the attached privacy policy. We will not share you information other than as described in the privacy policy. We will maintain and then delete your data as described.

We respect your rights under the GDPR and will always respond to requests to withdraw consent, forget your details, correct your details, stop processing or port your data as requested.

Important: You can object to processing, withdraw or amend your consent at any time, simply contact:

The Data Controller
Cheshire Companions
3 Grove Park Rd, Wrexham LL11 1DY
01614497775
info@cheshirecompanions.com

If you agree to the privacy policy and consent to us processing your data as described please provide signature and date below:

Signed	Date
• •	wwwe collect, process, and store your information. This is an ake time to read it. Please sign and date below to confirm that privacy statement
Signed	Date
End of document.	

