EMPLOYEE CONSENT AND PRIVACY POLICY TEMPLATES

Employee consent and privacy policy templates guidance

How should I use my employee consent and privacy policy templates?

GDPR regulates the way your company collects, stores and processes the data of individuals. The same rules apply to the way you use the personal data of your employees. The enclosed privacy policy template is designed to explain to employees how their data will be used, and the enclosed employee consent template gives them the opportunity to provide your company with explicit consent to use their data for the purposes outlined.

Will I need to update my employee consent and privacy policy templates?

Yes. You should review this document at least every 3 months and amend where necessary, to remain GDPR compliant.

Aims

Your company will need to collect certain personal information about the individuals working for it to carry out certain processes. This data could include information like health history, bank account details, marital status, home address and much more. As an employer, your company should go to great lengths to ensure that data is secure – and as a data controller adhering to GDPR rules, you have a range of legal obligations which apply to employee data.

To ensure your employees are informed about what data you're using, why you're using it and how it will be stored and processed, you should complete the enclosed employee privacy policy. Likewise, you should complete the enclosed employee consent template to collect the explicit consent of your employees, volunteers, contractors or anyone else associated with your company, stating that they agree for your company to collect, process and store their data.

Employee privacy policy template

Here at [COMPANY NAME] we take your privacy seriously. We greatly value your contribution to our success, and we will do everything we can to protect your individual rights and personal liberties.

As part of our ongoing relationship, we will need to collect, store and process certain information about you. This information is required to carry out certain processes, and we will clearly explain what those processes are and how your data will be used. You have the right to object to the processing of your data at any time.

This privacy policy may be occasionally updated in-line with company policy and regulatory updates. Any updates to this policy will be communicated to all employees as soon as possible.

How will your information be used?

As an employee of [COMPANY NAME], we must store and process information about you for management and administrative use only. The information you give us will be stored and processed only to allow us to maintain an effective relationship with you as an employee. These management processes apply during the recruitment process, whilst you are an employee for [COMPANY NAME] and when your relationship with our company has ended.

The management and administrative processes carried out using your data will allow us to adhere to the employee contract you have signed with us, as well as to comply with legal requirements we are duty-bound to follow. Your data may also be used to pursue the legitimate interests of [COMPANY NAME] and to maintain any established position in the event of legal proceedings.

Most of the information our company holds relating to you has been provided to [COMPANY NAME] by you. In some cases, we may also collect information about you from other internal sources such as a line manager. On other occasions we may collect and store information about you from external sources, such as a reference as part of the recruitment process.

If you don’t want to provide us with the information requested, [COMPANY NAME] might not be able to meet all of the obligations to you that we outlined in your employee contract. We will inform you in the event we are unable to comply with the conditions of your contract due to missing or withheld data.

We may anonymise your personal data in some cases so that it cannot be used to identify you. This may be done without notifying you.

After your relationship with our company has ended and you are no longer an employee at [COMPANY NAME], we will store and/or securely destroy the data we hold relating to you in-line with applicable regulations.

There may be limited circumstances in which your data must be transferred outside of the EU. This will only ever be done to comply with our legal obligations, or our company's contractual obligations to you as our employee. To protect your personal data, [COMPANY NAME] has implemented the following safeguards for data transfers:

- [List details here]
- [DETAILS]
- [DETAILS]
- [DETAILS]

Your personal data will be stored for a period of [PERIOD OF TIME], unless otherwise noted. Criteria used for determining data retention for other situations are as follows:

- [List details here]
- [DETAILS]
- [DETAILS]
- [DETAILS]

There may also be situations in which your data is used as part of automated decision-making processes. Examples of these processes include profiling activity, as well as:

- [List details here]
- [DETAILS]
- [DETAILS]
- [DETAILS]

Our legitimate interests

[COMPANY NAME] may occasionally need to process your data to pursue legitimate interests relating to our company and its business interests. Examples of situations in which we may process your personal data in the legitimate interests of the company include (but are not limited to):

- Fraud prevention
- Administrative purposes
- Crime reporting and detection

Our legitimate interests are [NATURE OF LEGITIMATE INTERESTS] in nature, and [COMPANY NAME] will never use your information or wilfully process your data in any situation in which your own interests outweigh the legitimate interests of our company. We process your personal data only within our rights as enshrined in law, and we do so in a way that is transparent and fair.

We may occasionally need to process your data to ensure it is accurate and up-to-date or to ensure it is safe and secure.

What information do we collect?

[COMPANY NAME] collects, stores and processes the following types of information about you as an employee:

- Your name
- Your title
- Your date of birth
- Your gender
- Your address
- Your telephone number(s)
- Your personal email address(es)
- Your marital status
- Information about dependents
- Your emergency contact information
- Your next of kin
- Your bank account details
- Your tax status information
- Your payroll records
- Your salary
- Information about your annual leave
- Your benefits information
- Your National Insurance number
- Your photograph
- Location of your employment or place of work
- A copy of your driving license
- A copy of your passport
- Your right to work documentation (if applicable)
- Your referees
- Your CV
- Your performance history
- Your disciplinary history
- Your grievance history
- CCTV footage (if applicable)
- Electronic key card records (if applicable)
- Information about your use of information systems

Why do we process your information?

[COMPANY NAME] may process your data for the following reasons:

- To make a decision about your appointment
- To carry out payroll processes

- To provide you with benefits
- To liaise with your pension provider
- To administer other elements of your contract
- To manage performance
- To carry out accounting and auditing functions
- To assess your qualifications for a particular project, task or promotion
- To make a decision about salary reviews
- To make a decision about your continued employment
- To gather evidence about grievance or disciplinary hearings
- To address legal disputes
- To make a decision about terminating our relationship
- To assess your education or training requirements
- To manage your absences
- To ascertain your fitness to work
- To comply with health and safety obligations
- To carry out equal opportunities monitoring
- To prevent fraud
- To ensure network and information security
- To conduct data analytics

It is inevitable that in your capacity as an employee you will be referred to in company records. Please also note that wherever necessary, [COMPANY NAME] may need to keep information relating to your health, such as reasons for absence and evidence of GP notes. This information will only ever be used to comply with our health and safety obligations and to administer benefits such as statutory sick pay or [ADD BENEFITS].

If we need to process special categories of data, we will always obtain your explicit consent and explain for what purpose this information must be processed, unless this information is required to protect your health in an emergency, or if consent is not required by law.

Special categories of information may include (but are not limited to):

- Sexual orientation
- Racial or ethnic origin
- Political affiliations
- Religious affiliations
- Trade Union membership
- Biometric data

Where consent is given to process this information, you reserve the right to withdraw your consent at any time.

We will only ever disclose information about you to external parties if [COMPANY NAME] is legally obligated to do so, or in situations in which we must disclose your information to comply with our company's contractual obligations to you. Examples may include passing your

contact details onto your pension provider. We may also transfer information about you to other companies within our wider family of companies, for purposes related to your employment or purposes related to company management and administration.

We may occasionally rely on profiling and/or automatic decision-making. This will only be used in certain limited situations, [INSERT DETAILS OF THESE SITUATIONS] [INCLUDE INFORMATION ABOUT THE REASONS, IMPACT AND POTENTIAL CONSEQUENCES OF PROCESSING DATA USING AUTOMATED DECISION-MAKING].

We also monitor computer and telephone usage, to ensure that employment activities are carried out in-line with our Data Protection Policy and the Company Handbook.

To perform our contract with you or adhere to our legal requirements, your information may be transferred outside the EU or to global organisations. To ensure your data is protected, we have a list of security measures [LIST SECURITY MEASURES]. A copy of these security measures can be requested from [INSERT HERE].

We will store your personal information for a period of [INSERT PERIOD HERE]. We will also rely on the criteria outlined in the retention schedule when deciding how long to store your information. If we decide to store your personal information for a new reason, or a reason which differs from the one it was originally collected and stored for, the Data Protection Officer will provide you with this reason and any other accompanying information.

What are your rights?

[COMPANY NAME] observes a host of regulatory obligations under the EU's GDPR legislation and the Data Protection Act 2018. As part of our ongoing commitment to preserve and uphold these regulatory commitments, we will also uphold your personal rights under these regulations.

Your statutory rights under GDPR and the Data Protection Act 2018 include:

- The right to request access to your personal information (also known as a 'data subject access request')
- The right to request corrections be made to the data we hold about you
- The right to request erasure of your personal data
- The right to object to the processing of your data
- The right to request any restrictions to the processing of your data
- The right to request the transfer of your data to another party

If you would like to exercise any of these rights, please contact [NAME OF DATA PROTECTION OFFICER] in writing at [COMPANY ADDRESS OR EMAIL ADDRESS OF DATA PROTECTION OFFICER].

You do not need to pay a fee to access the personal data we hold on you to exercise your rights under relevant data protection regulation; however, [COMPANY NAME] reserves the legal right to charge a nominal fee for requests that are deemed to be unfounded or excessive in nature. We may also refuse to comply with requests that are deemed unfounded or excessive in-line with our own legal rights.

Please note that [COMPANY NAME] may be required to collect more information about you to confirm your identity, before granting access to any information requested.

You have the right to issue a formal complaint to the Information Commissioner's Office at any time, if you feel [COMPANY NAME] has not adequately complied with its requirements under GDPR or the Data Protection Act as they relate to the collection, storage, processing of your personal data, or your individual rights to access your data.

Who is [COMPANY NAME]'s Data Protection Officer?

[COMPANY NAME] is the controller and processor of data. We collect, store and process data in accordance with our legal obligations under GDPR and the Data Protection Act 2018.

If you have any questions or concerns relating your information and the way we use it, please get in touch:

[DATA PROTECTION OFFICER NAME]
[DATA PROTECTION OFFICER EMAIL ADDRESS]
[COMPANY NAME]
[COMPANY ADDRESS OR WEBSITE URL]

Signature _____ Date _____

Employer GDPR checklist

Complete this checklist to confirm you have reviewed your contracts and other documentation to include the relevant privacy notice and consent forms.

Action	Complete	Notes
Employee information audit		
Identify what personal data you hold on employees and where it originated from		
Identify how your company will process personal data and for what purposes the data is being processed		
Verify retention periods and review		
Identify any third-parties your company must transfer data to and outline reasoning		
Conduct a review of associated contracts		
Identify any situations in which automated decision-making could be used		
Document audit		
Identifying lawful basis for processes data		
Obtain employee consent		
Confirm status for processing sensitive personal data		
Identify lawful basis for processing employee personal data (one of the following must apply)		
Employee must give valid consent		
Processing activity required to carry out delivery of contract		
Processing activity necessary to comply with legal obligation		
Processing activity necessary to serve vital interests of individual or others		
Processing activity necessary to serve public interest		
Processing activity necessary to serve legitimate interests of the company (note the legitimate interests of the company can and will be overridden by the individual rights of the data subject)		
Identify lawful basis for processing special categories of personal data (one of the following must apply):		
Explicit consent		
Processing activity required to comply with employment rights		
Processing activity necessary to serve vital interests of individual or another if individual cannot give valid consent		

Processing by a foundation, association or not-for-profit with a political, philosophical, religious or Trade Union aim		
Situation in which employee has made data public		
Processing activity necessary for legal action		
Processing activity necessary to serve public interest		
Processing activity necessary to assess employee's work capacity		
Identify lawful basis for processing personal data relating to criminal convictions		
Processing activity must be authorised under UK and EU law		
Explicit consent		
Processing activity necessary to serve vital interests of individual or another if individual cannot give valid consent		
Processing by a foundation, association or not-for-profit with a political, philosophical, religious or Trade Union aim		
Situation in which employee has made data public		
Processing activity necessary for legal action		
Data cleansing		
Update retention policy		
Securely delete or de-personalise data		
HR policies and procedures		
Amend procedures relating to recruitment, promotions, compensation, disciplinary, grievances, performance management, sickness absence, employee monitoring and references.		
Conduct a data protection impact assessment (if applicable).		
Notify employees of any relevant changes to employee handbook or corresponding manuals.		
Automated decision-making		
Identify lawful basis that enable you to make decisions based on automated processing		
Automated decision-making necessary to carry out delivery of contract		
Notify employees of a decision based on automated processing (and allow right to request a reconsideration within 21 days of notification)		
Explicit consent		
Implement suitable safeguards to defend employee rights		
Automated decision-making concerning special categories of personal data must include explicit consent unless processing is in the public interest		

Data transfers to third parties		
Identify lawful basis for data transfers		
Implement processor agreements where applicable		
Update procedures		
Notify employees of processing		
Draft an updated privacy policy for employees		
Ensure all procedures are up-to-date		
Data subject rights		
Update Subject access request policy and procedures		
Arrange training for all employees handling subject access requests		
Develop company procedures for the handling of employee rights		
Data protection officer		
Find out whether you need to appoint a data protection officer		
If applicable, appoint a data protection officer		
If a data protection officer is not required by law, appoint a senior management figure to handle data protection issues		
Review		
Arrange training for all employees responsible for handling data		
Ensure all processes and policies are scheduled for regular review		

Employee consent template

Here at [COMPANY NAME] we value your privacy. As part of our relationship with you, our company will be required to collect, process and store certain information about you. This information may include your personal details, information about your family, employment history, medical conditions or any other information we have outlined in our employee privacy policy.

We will never share your information with any individual or company other than those listed within our employee privacy policy, and wherever possible we will always uphold your right to withdraw consent or to remove data.

You can withdraw your consent, amend your consent or object to processing at any time by contacting:

[INDIVIDUAL NAME]
[COMPANY NAME]
[COMPANY ADDRESS]
[COMPANY PHONE]
[COMPANY EMAIL]

Please sign and date below to verify you have read and understand the enclosed employee privacy policy and that you consent to [COMPANY NAME] processing your data as described within this policy.

Signature _____ Date _____