

**GDPR TEMPLATE:**

**EMPLOYEE DATA RETENTION PROCESS**

**Points to note**

* Before using this template Employee Data Retention Process, it is essential that you read these ‘Points to note’, together with the separate document, ‘Make UK Essential GDPR Templates for HR – Points to note’, which provides important information applicable to all of the template documents, including the Employee Data Retention Process.
* This template Process has the following purposes:
  + It is designed to help ensure your compliance with the GDPR requirement to hold Employees’ and Job Applicants’ (both as defined in the body of the document) personal data for **no longer than necessary for the purposes of processing.** The Process is an organisational measure which ensures and demonstrates compliance with this obligation, including a section on applicable retention periods as well as details of how to apply these in practice.
  + ‘Where possible’, you need to record in your Record of Processing the envisaged time limits for erasure for the different categories of personal data held. This template Process sets out these envisaged time limits/retention guidelines and the GDPR Template: Employee Record of Processing refers out to this document.
  + As this template Process explains your policies as regards the retention and erasure of personal data, we think it can operate as one element of the ‘appropriate policy document’ required under the Data Protection Act 2018 (DPA 2018) as an additional safeguard for processing special category data (and data relating to criminal offences or convictions) in certain circumstances.
  + Another of the DPA 2018’s additional safeguards for processing special category data (and data relating to criminal offences or convictions) in certain circumstances is the requirement to state in your Record of Processing whether or not such data is retained and erased in accordance with an ‘appropriate policy document’ and, if it is not, to explain why not. Provided that this Process is applied in practice, it should, we think, enable you to state in your Employee Record of Processing that the relevant special category data/criminal offences/convictions data *is* retained and erased in accordance with an ‘appropriate policy document’ (i.e. this Process).
* This template Process deals with the retention and erasure of personal data relating to Employees and Job Applicants. It does not cover other types of personal data that may be held and used by the company, for example it does not cover customer or marketing personal data. Companies will need to have other processes in place to cover the retention and deletion of such personal data.
* This template Process is not designed to be given to all Employees – it is ‘role specific’. It is directed at and intended for use by HR, managers, and other employees who have particular responsibility for handling Employee and Job Applicant personal data. You will need to decide which of your employees to give it to.
* The first part of this template Process, **Retention Periods for Employee and Job Applicant Personal Data**, explains the approach to setting retention periods.
* This Process sets out and explains the criteria (referred to in the Process as ‘Employee Data Retention Criteria’) that you should take into account when:
  + setting the retention periods for Employee and Job Applicant personal data;
  + determining how long to keep particular items of Employee and Job Applicant personal data where you have specified that the retention period for a given category of personal data will be decided on a ‘case by case’ basis; or
  + it is necessary to depart from one of the retention periods that you have specified in the Appendix to this document (referred to as ‘Retention Periods’).
* The content of the Employee Data Retention Criteria also appears in the GDPR Templates: Employee and Job Applicant Privacy Notices and in the GDPR Template: Data Protection Policy. If you customise the Employee Data Retention Criteria in this Process, you will also need to make consequential changes to the relevant sections of those documents.
* Use the placeholder table for Retention Periods in the Appendix to this Process to set out the appropriate retention periods that you have been able to identify, but note that it is unlikely that you will be able to identify a specific retention period for *each and every* *type or* *item* of Employee personal data that you hold and process. You may wish to add an extra column to the table to list known locations for the different categories of personal data (which could include archived data) if you have this information available, as it may assist you when you come to delete personal data once the Retention Periods have expired.
* There is no ‘one size fits all’ when it comes to setting an organisation’s Employee and Job Applicant data retention periods for the purpose of GDPR compliance and the approach taken by organisations will vary. Each employer must consider the issue in the context of its own business requirements/operations and make its own decisions about the retention periods that it considers are suitable. For some *example* retention periods that a company *might* choose and a table of common statutory retention periods (i.e. where the law says you must retain records for a specified period), see ‘*Accompanying document to GDPR Template: Employee Data Retention Process – Example retention periods*’.
* We recommend that you incorporate any applicable statutory retention periods into your Retention Periods that you include in the Appendix rather than presenting them separately, so that HR/managers do not have to look in two different places to find the applicable retention period for a particular item of Employee or Job Applicant personal data.
* The GDPR Template: Employee Privacy Notice includes information for Employees about the periods for which data are retained (or, if that is not possible, the criteria used to determine the periods). However, we recommend that you drill down from the **long-stop** retention periods for **broad categories** of Employee personal data that are listed in the Appendix to the Employee Privacy Notice (referred to as ‘Guideline Retention Periods’). Simply applying these long-stop periods to all information that falls within these broad categories is likely to result in you keeping particular items of Employee personal data for longer than is necessary. For strict compliance in practice with your obligation to keep personal data for no longer than is necessary, individuals who have responsibility for Employee personal data should apply more granular retention periods. For example:
  + Employees may be told in the Employee Privacy Notice that personal data falling within the category of ‘disciplinary, conduct and grievance matters’ will be held for up to 6 months after employment ends. In this Process, it would be helpful to identify shorter retention periods for some types of data falling within this category, such as expired disciplinary warnings, or disciplinary allegations which are not taken forward.
  + Employees may be told in the Employee Privacy Notice that the retention periods for ‘sickness absence and medical information’ will be determined on a case by case basis, by reference to the applicable criteria. However, in this Process, you may be able to set retention periods for specific items of data such as self-certificate forms, SSP records, and attendance review cautions.
  + Employees may be told in the Employee Privacy Notice that the retention periods for the ‘health and safety’ category of personal data are decided on a case by case basis. However, in this Process, you could set out retention periods for records of reportable accidents and other any records that you are obliged to maintain under legislation relating to exposure to hazardous substances.
* To avoid confusion, the Process includes a paragraph which explains why there are differences between the Guideline Retention Periods in the Employee Privacy Notice and the Retention Periods in this Process.
* In addition, guidance from the Information Commissioner’s Office specifies that an ‘appropriate policy document’ (which the DPA 2018 requires you to have in place in order to process special category data in certain circumstances) should indicate how long you are likely to retain each type of special category data to which the appropriate policy document requirement applies. As noted above, this Process is intended to operate as one element of the appropriate policy document; this provides another reason why we recommend setting more granular retention periods in this Process than the Guideline Retention Periods set out in the Employee Privacy Notice.
* Note that this Employee Data Retention Process is intended to cover personal data belonging to Job Applicants, as well as Employees. We do not think it is necessary to have a separate retention process for Job Applicants’ personal data, as the general principles applicable to such data are the same. However, when completing the table in the Appendix to this Process, we recommend you include a Retention Period for the personal data of Job Applicants whose applications are unsuccessful, who turn down a job offer, or who submit speculative or unsolicited applications. When doing so, bear in mind that, unlike for personal data belonging to Employees:
  + You should not need to break down the broad categories of personal data described in the Job Applicant Privacy Notice in order to set more granular retention periods for particular items of Job Applicant personal data. Instead, you could apply a single retention period to *all* personal data belonging to unsuccessful / speculative Job Applicants, or those who have turned down a job offer. However, if it is your practice to retain Job Applicants’ personal data on file for consideration for future vacancies, this will need to be reflected in your Retention Periods (i.e. you should set a basic period for which you retain all Job Applicants’ personal data, and a longer period that will apply where a Job Applicant has agreed to you keeping their personal data on file for this purpose).
  + The possible Guideline Retention Periods we have suggested in the template Job Applicant Privacy Notice are sufficiently short that applying them should not generally result in you keeping Job Applicants’ personal data for longer than necessary. Accordingly, the Retention Periods you set out in this Process could simply reflect what you tell Job Applicants in the Job Applicant Privacy Notice about how long you will keep their personal data.
* Keeping personal data “just in case” it might be relevant to a future legal claim or a complaint will often result in personal data being held for longer than is necessary. This Process therefore assumes that it is company policy that risk-based assessments as to whether or not a claim/complaint is likely should be made in individual cases and that the Retention Periods in the Appendix reflect this approach. If this is not your approach, you will need to amend this section. The Process provides for the possibility of overriding/departing from the Retention Periods where, for example, an individual has complained about an issue or has otherwise behaved in a way that indicates that they might make a complaint or bring a legal claim in the future, or you are aware that they could complain about action you have taken.
* The second part of this template Process, **Retention and erasure in practice**, sets out high level principles for what is expected of HR, managers and employees with particular responsibility for Employee and Job Applicant personal data. It will need to be tailored to reflect the reality of your own operations and it assumes that there will be more detailed supporting processes in place in relation to particular activities. You may also need to refer to any relevant company policies. Note the following:
  + This Process includes provision for Employee personal data to be regularly reviewed to ensure that it remains relevant and is not retained for longer than necessary. Methods of review will necessarily differ from organisation to organisation so, while we have provided suggested wording in square brackets, this will need to be tailored to reflect the processes that you have/can put in place in your organisation. You should also include details of any more specific processes you may have as a company concerning the periodic deletion of Employees’ personal data (e.g. if you have an online HR Portal that is configured to automatically delete certain records/flag them for deletion after a specified time limit has expired).
  + Make UK recommends undertaking a data cleansing exercise in relation to former Employees’ data six months after they have left employment to ensure that all personal data has been deleted**, except for** personal data that must be retained in order to comply with a statutory retention obligation, or that you still legitimately require in accordance with the guidelines set out in this Process. This template Process provides for such data cleansing and includes a placeholder for you to insert details of how such an exercise will be managed in practice in your organisation. The paragraph, ‘**What about possible legal claims by Employees?**’,also refers to data cleansing six months after an individual has left employment andmakes specific reference to the need to identify whether there is a real risk of a claim/complaint – in which case, the relevant data should be retained for longer. If you do not intend to data cleanse six months after an individual has left employment, then you should amend this section accordingly.
  + This Process includes provision for deleting/destroying Employee and Job Applicant personal data. Instructions for deletion will necessarily vary depending on your organisation’s particular systems and practices and you will need to insert details accordingly.

**Employee Data Retention Process**

**Introduction**

Data protection law prohibits [COMPANY] from keeping information (personal data) about our staff for longer than is necessary for the purposes for which we use it. [COMPANY’S] Data Protection Policy [, *which is available from/LINK,*] explains this obligation and sets out the general principles we expect you to follow in relation to the retention and erasure of personal data.

This Employee Data Retention Process, which supports the Data Protection Policy, deals with the retention and erasure of personal data about current and former employees, workers, [contractors, agency workers, consultants, interns, volunteers, partners and directors], (together referred to as ‘Employees’) and about individuals who have applied to work for [COMPANY], whether as an employee, worker, [contractor, consultant, intern, volunteer, partner or director] (together referred to as ‘Job Applicants’). It sets retention periods for Employee and Job Applicant personal data (and criteria to be taken into account when deciding on how long to keep data) and explains what we expect you to do to ensure that Employee and Job Applicant personal data is deleted or destroyed at the appropriate time and in a secure way.

This Process applies to all employees with particular responsibilities for the retention and erasure of personal data (and who will be informed of such by [COMPANY]). You are expected to familiarise yourself with and follow this Process. Failure to do so could lead to disciplinary action and, in serious cases, termination of your employment. Please note that we may update this Employee Data Retention Process at any time.

**Why is data protection compliance important?**

Failure to comply with data protection law – including obligations relating to the retention and erasure of personal data – may cause harm to individuals and expose [COMPANY] and, in some cases, individual Employees to serious legal liabilities. These can include criminal offences and fines of up to £17.5million or 4% of total worldwide annual turnover, whichever is higher. In addition, an individual may seek damages from us in the courts if we breach their rights under data protection law. Breaches of data protection law can also lead to serious damage to our brand and reputation.

**Retention periods for Employee and Job Applicant personal data**

Where possible, we have indicated how long [COMPANY] should retain identified categories, types or items of Employee and Job Applicant personal data in the ‘**Retention Periods**’ in the Appendix to this Process. When deciding on these periods, we took into account the following criteria (‘**Employee Data Retention Criteria**’):

* the amount, nature, and sensitivity of the personal data;
* the risk of harm from unauthorised use or disclosure;
* the purposes for which we process the personal data and how long we need the particular data to achieve these purposes;
* how long the personal data is likely to remain accurate and up to date;
* for how long the personal data might be relevant to possible future legal claims (for more details, see below); and
* any applicable legal, accounting, reporting or regulatory requirements that specify how long certain records must be kept.

We expect you to apply the Retention Periods set out in the Appendix to this Process most of the time. However, occasionally situations may arise which mean that you should retain Employee or Job Applicant personal data for a longer or shorter period than the applicable Retention Period, taking into account the Employee Data Retention Criteria listed above. For example:

* The Retention Period for records and correspondence relevant to family leave taken is [*12 months following return to work from applicable leave*] but, if you were involved in an ongoing tribunal claim of pregnancy discrimination with an Employee when the Retention Period expires, it would clearly be appropriate for you to retain that data for longer.
* The Retention Period for bank details is [*6 months after employment ends*], but if a current Employee switches banks and provides new bank details, since the old bank details have been replaced, they should be deleted [*within 6 months*] following the change.
* The Retention Period for all Job Applicant personal data is [*6 months*] after you have informed a Job Applicant that their application has been unsuccessful but, if the Job Applicant were to lodge a tribunal claim alleging that the interview panel was biased against them due to their race, it would be appropriate to retain their personal data for longer so that you can properly defend the claim.

Employee or Job Applicant personal data may also be retained for a longer or shorter period than the applicable Retention Periods where it is held on IT back-up data sets that are produced for disaster recovery purposes. This is because it may not be possible to apply the Retention Periods to individual records without erasing the whole back-up data set. [Back-up data sets are generally retained for up to [3 years] for disaster recovery purposes.]

Where no Retention Period is specified for a particular category, type or item of Employee personal data (i.e. we have provided that it will be assessed on a case by case basis), the appropriate period should be decided by considering the Employee Data Retention Criteria. Sometimes you may also find it a helpful starting point to look at the indicative ‘long-stop’ Guideline Retention Period for the relevant broad category of Employee personal data that is set out in the Employee Privacy Notice [*available here: LINK*]. (For more detail, see **Why are the retention periods in the Employee Privacy Notice longer?**)

If you are unsure of the appropriate retention period in a given circumstance, and/or are considering departing from the Retention Periods, you should contact [the Data Protection Officer/Data Protection Team/HR Data Protection Lead] for guidance, via [*insert contact details*].

**Why are the retention periods in the Employee Privacy Notice longer?**

Data protection law requires us to inform Employees and Job Applicants how long we retain their personal data or, if this is not possible, to tell them what criteria we use to determine how long we will keep it. We do this in our Employee Privacy Notice [*available here: LINK*] (and, for Job Applicants, our Job Applicant Privacy Notice [*available here: LINK*]).

You will notice that some of the Guideline Retention Periods listed in the Employee Privacy Notice differ from the Retention Periods set out in the Appendix to this Process. This is because the Guideline Retention Periods in the Employee Privacy Notice relate to broad categories of Employee personal data to keep that document as user-friendly as possible for all Employees, whereas the Retention Periods in this Process break down these broad categories of personal data into more detailed subsets of data. In addition, the Guideline Retention Periods in the Employee Privacy Notice are intended to inform Employees of the *longest* period for which we will generally hold their personal data, whereas it will often be appropriate to delete or erase certain items of personal data before this long-stop date. Where possible, this is reflected in the Retention Periods in this Process.

The above does not apply in respect of Job Applicant personal data, for which the Retention Periods set out in the Appendix to this Process match what Job Applicants are told in the Job Applicant Privacy Notice. This is because we hold more limited personal data about Job Applicants than we do about Employees, and the Guideline Retention Periods described in the Job Applicant Privacy Notice are short enough that, ordinarily, we will keep Job Applicant personal data throughout the relevant period.

**What about possible legal claims by Employees and Job Applicants?**

There is an understandable temptation to keep hold of Employee and Job Applicant personal data in case it may be relevant to a legal claim or complaint that an Employee or Job Applicant may one day seek to bring against the Company. You may therefore find the following information about legal limitation periods useful:

* Most employment tribunal claims, e.g. unfair dismissal, discrimination etc., have time limits of three months, or occasionally six months. However, these time limits can be ‘extended’ in practice by virtue of Acas Early Conciliation, and the operation of judicial discretion may allow an extension of a statutory time limit in certain circumstances.
* Workplace personal injury claims usually have a three year time limit (although, in relation to industrial diseases, the time limit does not generally start to run until an individual is aware they have a particular disease/condition).
* Breach of contract claims in the courts have a six year time limit (as do equal pay claims).

The Retention Periods in the Appendix take into account our policy not to keep Employee and Job Applicant personal data “just in case” it might be relevant to a future legal claim or a complaint; instead, we ask that risk-based assessments should be made in individual cases, focusing on whether there is a real risk that the Employee or Job Applicant in question could bring a claim or make a complaint in the future.

If, in a given circumstance, you think there is **a genuine risk that an Employee or Job Applicant might bring a legal claim or make a complaint in the future** (and the limitation period for the possible legal claim expires after any relevant Retention Period), it may be appropriate to keep relevant personal data for longer than the applicable Retention Period. [In particular, if you are carrying out a data cleansing exercise [*six months*] after an Employee has left employment, you should consider whether, in the individual circumstances and based on the Employee’s employment history, there is a real risk of a legal claim or complaint such that it is necessary to depart from the Retention Periods.]

[For example, the Retention Periods provide that it will only be necessary for details of Employees’ contract terms to be retained for [*up to 6 months after employment has ended*]. Suppose that an ex-Employee complains about the non-payment of a bonus due in their notice period and you therefore consider that there is a genuine risk of them bringing a breach of contract claim. In these circumstances, it may be appropriate to depart from the Retention Period and to keep personal data relevant to that bonus decision for six years.]

If, in a given circumstance, you are considering departing from the Retention Period or are unsure about the risk or impact of a possible legal claim or complaint on how long you should retain particular personal data, you should contact [the Data Protection Officer/Data Protection Team/HR Data Protection Lead] for guidance, via [*insert contact details*].

**Retention and erasure in practice**

**Instructions and training**

You are expected to follow this Process and any other instructions or training you are given relating to the retention and deletion of Employee and Job Applicant personal data from time to time.

HR or managers responsible for a particular work-stream or activity involving Employee or Job Applicant personal data must remind relevant team members about their obligations in relation to the retention and deletion of the data as appropriate.

**Storing personal data in easy to find locations and minimising unnecessary copies**

You should follow any protocols, instructions or training relating to the storage of Employee and Job Applicant personal data and the minimisation of unnecessary copies.

If Employee and Job Applicant personal data is stored in easy to find locations, then it is much easier to review and, consequently, easier to delete at the appropriate time. Storing Employee and Job Applicant personal data in as few places as possible not only avoids the possibility that duplicate copies are not updated and become out of sync, but also reduces the risk that additional copies are retained after the central document has been deleted. You should work from and update a single central copy where possible. [For example: *Insert details, e.g.* Employee documents and records should be stored on the HR portal only, and not on your own computer.]

If you do print or save your own copies of documents containing Employee or Job Applicant personal data while you are dealing with a relevant issue, [including on any BYO device,] you should delete or destroy these when your involvement with the issue has ended and the most up-to-date/final version of the relevant record has been stored in the appropriate central location, e.g. [saved on the HR Portal]. [For example, a manager carrying out a performance appraisal may print out a paper copy of a performance appraisal form for use in the appraisal meeting. When the final record of the appraisal meeting is saved [on the HR Portal], the manager should destroy their printed copy.]

**Reviewing current Employees’ personal data on a regular basis**

Regular reviews of Employee personal data help to ensure that personal data is not retained longer than is necessary for the identified purposes.

[*Insert details of who is responsible for reviewing key processes or locations, for example:* HR is responsible for conducting regular reviews of current Employees’ personnel files to ensure that the personal data they contain remains relevant and is not retained for longer than necessary. / Line managers are responsible for ensuring that they review the Employee personal data they store in hard and soft copy on a quarterly basis.]

[*Insert details of any more specific processes that you operate to ensure that current Employees’ personal data is not retained for longer than necessary.* *For example*: Personal data stored on the holiday booking system is deleted automatically after [*insert time period*].]

**Data-cleansing for former Employees and Job Applicants**

The Retention Periods in the Appendix provide that a significant amount of Employee personal data should be deleted [*6 months*] after an Employee stops working for us, and that Job Applicant personal data should be deleted [*6 months*] after we have informed a Job Applicant that their application has been unsuccessful or a successful Job Applicant has rejected a job offer from us [(unless they have agreed to us keeping their personal data on file for consideration for future vacancies)].

[*Add specific details, for example:* HR are responsible for undertaking a data cleansing exercise in relation to an Employee’s personal data held [on the HR Portal/in the Employee’s personnel file] [six months] after they have stopped working for us./ Line managers are responsible for undertaking a data cleansing exercise in relation to an Employee’s personal data held within their team/department [six months] after they have stopped working for us./ IT are responsible for carrying out a data cleansing exercise in relation to the Employee’s personal data held on any IT equipment they have returned [one month] after the Employee has stopped working for us].

When carrying out a data cleansing exercise, remember to consider if there is a genuine risk of a legal claim or complaint in the particular circumstances as you may need to depart from the Retention Periods if there is (see **What about possible legal claims by Employees and Job Applicants?**).

**Deleting/destroying Employee and Job Applicant personal data securely**

Employee and Job Applicant personal data must be deleted or destroyed securely in accordance with the [Information Security Policy] [and [*refer to other relevant policies, such as the Technology and Communications Policy*]].

In particular, you must [*Insert instructions explaining any applicable processes for the deletion of Employee and Job Applicant personal data. This should include, for example, instructions concerning:*

* *securely shredding hard copy files;*
* *deleting electronic records from online HR portal or other centralised database, deleting back-up records, etc.;*
* *deleting personal data from electronic devices (including removable storage devices) when it is no longer required (this means not simply deleting files, but also emptying the recycle bin on your desktop/ laptop/tablet/other devices as applicable);*
* *ensuring personal data is wiped from redundant devices e.g. old laptops, mobile phones, memory sticks, performance output data from redundant machinery, etc.;*
* *removing personal data from software, applications, intranet, etc.;*
* *deleting individually held paper and electronic copies of personal data;*
* *following company instructions about the deletion of emails;*
* *requiring departing Employees to return all company property that may contain any personal data and securely dispose of any hard copies*].

**[*Include if you use electronic or hard copy archiving:* Archiving**

Archiving or moving Employee and Job Applicant personal data to storage locations which are less easily accessed can be a good way of ensuring that the personal data is only shared on a need to know basis. However, when considering moving Employee or Job Applicant personal data to electronic or hard copy archive, have regard to the Retention Periods in the Appendix and only archive what is really necessary. Consider whether you could delete the Employee or Job Applicant personal data instead. If you do archive Employee or Job Applicant personal data, ensure that you delete remaining versions/copies.]

**Requests to access, correct, erase or exercise any other individual rights in relation to personal data**

If you receive a request from any current or former Employee or Job Applicant who wishes to access, correct, erase or exercise any other rights in relation to their personal data, you should immediately refer the request to [the Data Protection Officer/Data Protection Team/HR Data Protection Lead] for guidance, via [*insert contact details*].

Once you are aware of an access request, you must not do anything to prevent the individual from receiving information they would be entitled to in response to their request. For example, you must not amend, delete or hide personal data that relate to the request, unless you would have done this in any event in the absence of a request. If you are unsure, you should contact the [Data Protection Lead/Data Protection Officer/Data Protection Team] before taking any action. Failure to comply with this instruction could lead to disciplinary action (including dismissal) as well as criminal liability.

**Appendix: Retention Periods for Employee and Job Applicant Personal Data**

This table sets out [COMPANY]’s identified Retention Periods for Employee and Job Applicant Personal Data. Please refer to the body of the Employee Data Retention Process for information on how these Retention Periods were determined and guidance on when it may be appropriate to depart from them.

|  |  |  |  |
| --- | --- | --- | --- |
| **Specific type of personal data** | **Retention Period** | **Additional information / explanation** | **[*Optional – see ‘Points to note’:* Location of personal data]** |
| *[Complete as appropriate for your organisation.*  *E.g. Annual performance appraisal documentation]* | *[Complete as appropriate for your organisation.*  *E.g. Two years]* | *[Complete as appropriate for your organisation.*  *E.g. Required for performance assessment and comparison purposes, and for consideration in redundancy situation (in accordance with company redundancy procedure) and applications for internal promotion]* | *[Complete as appropriate. Include archived information]* |
| *[Complete as appropriate for your organisation.*  *E.g. Statutory maternity pay records]* | *[Complete as appropriate for your organisation.*  *E.g. Three years after the end of the tax year in which the maternity pay period ends]* | *[Complete as appropriate for your organisation.*  *E.g. Statutory Maternity Pay (General) Regulations 1986, Reg 26]* | *[Complete as appropriate. Include archived information]* |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |