How CIPHR’s products can help you meet your requirements for GDPR compliance

A guide to the tools available in CIPHR and CIPHR iRecruit
CIPHR is a leading UK-based developer and provider of HR software as a service (SaaS), offering a scalable solution that covers the entire employee lifecycle. Our systems’ features include people management, employee self service, absence and working time management, payroll, online recruitment, communications and reporting, and can be tailored to suit your organisation’s specific requirements.
Introduction

The General Data Protection Regulation (GDPR), which comes into force on 25 May 2018, is the biggest change to UK data protection law since 1998.

It has significant ramifications for how organisations collect, store and use personal information about customers and contacts, as well as for data about their employees, staff, volunteers, job applicants, and alumni.

Organisations that don’t take the proper steps to comply with the regulations may be liable to hefty fines that, in the most severe cases, could reach €20 million or 4% of turnover.

The GDPR sets out six lawful bases under which an organisation can process an individual’s personal data. The ICO defines these as:

1. **Consent**: the individual has given clear consent for you to process their personal data for a specific purpose
2. **Contract**: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract
3. **Legal obligation**: the processing is necessary for you to comply with the law (not including contractual obligations)
4. **Vital interests**: the processing is necessary to protect someone’s life
5. **Public task**: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law
6. **Legitimate interests**: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual’s personal data which overrides those legitimate interests

It is up to employers (the data controller) to determine which lawful basis applies for each usage of employee’s and applicants’ personal information.
The GDPR also sets out eight rights for individuals for their data:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

This guide will explore how tools made available in CIPHR and CIPHR iRecruit can be configured to meet the requirements that you have determined you need to put in place to comply with the data-protection rights of current staff and volunteers, former staff and volunteers, and job applicants.
Tools available in CIPHR to assist with GDPR compliance

CIPHR’s existing functionality enables HR teams to comply with the requirements of the GDPR. But we have also developed a number of additional tools that can make it even easier for you to comply with the regulations. Please contact your account manager to discuss activating any or all of these additional tools.

**Tool: GDPR dashboard**
**Helps you comply with: right to erasure, right to restrict processing**

A new dashboard is now available in CIPHR that makes it easy for you to identify data that needs to be deleted or anonymised, such as when staff or volunteers leave your organisation.

You can choose to delete or anonymise records individually or in bulk.

Choosing to anonymise data means personally identifiable fields will be removed. This will enable you to continue to report on non-personally identifiable information, such as anonymous absence records, for management information purposes, while remaining compliant with the GDPR. The ability to anonymise records in CIPHR is only available through the GDPR dashboard.
The dashboard also helps you to report on the number of records whose removal is overdue, by different segments of your organisation. Other reporting tools in CIPHR will help you to report on the different facets of the personal data held in your system, such as if consent has been gained to hold details about an employee's contacts.

Figure 1: example of GDPR dashboard in CIPHR

To add the GDPR dashboard to your system please contact your account manager on 01628 814 060 or email cm@ciphr.com.
**Tool: policy acceptance**  
**Helps you comply with: right to be informed**

Use CIPHR’s policy acceptance function – which alerts staff to documents they need to read, and requires them to confirm they have read the information – to help keep staff informed about the information you hold about them, your data retention periods, and how you will use their personal details. By using this function, you’ll create and maintain a robust, auditable record of what information has been communicated to staff and when.

---

**Tool: add additional user to CIPHR**  
**Helps you comply with: all rights**

You can choose to add an additional user to CIPHR – such as a GDPR administrator – with restricted access to only screens, fields and records associated with GDPR compliance. This means that if you have a dedicated employee or employees for GDPR compliance, outside the HR team, they can take care of their duties without having to ask HR for assistance with CIPHR.

---

**Tool: define data retention periods**  
**Helps you comply with: right to erasure**

In CIPHR you are now able to define data retention periods for staff and volunteers who leave your organisation. It is up to you to decide and set the retention period – whether that’s 30, 60, 90 days or more.

Different retention periods can be set for different subsets of your staff and volunteers, such as those working in other countries, if necessary.

---

**Tool: CIPHR offboarding**  
**Helps you comply with: right of access, right to data portability**

Individuals have the right to submit subject access requests (SARs) to organisations to find out what data they hold about them. These requests previously cost the individual £10 per request but are now free of charge. Organisations must comply with the request within 30 days, unless the request is deemed to be particularly complex.

You can now choose to manually reactivate access for an alumnus to CIPHR offboarding so they can securely view and download personal data your organisation holds about them, in response to a SAR.
Tool: CIPHR self-service
Helps you comply with: right of access, right to rectification

CIPHR’s standard employee self-service functionality enables staff and volunteers to see what data your organisation holds about them, and update or amend it as necessary. This self-service access is in line with good practice recommendations from the ICO about complying with the rights to access and to rectification.

Tool: contact consent record and automatic notifications
Helps you comply with: right to be informed

You can choose to add a field to an employee’s contact’s record (such as next-of-kin or emergency contacts) to indicate the date on which consent was given. You can also choose to set up automatic notifications to these contacts to reconfirm their consent, or to contact employees to ask them to reaffirm consent, on a schedule chosen by you.

To add the ‘consent given’ date field to contact’s records please contact CIPHR’s service desk on 01628 814 040 or email servicedesk@ciphr.com.
Upgrades to CIPHR iRecruit to assist with GDPR compliance

Your data protection obligations under GDPR extend not only to your current and former employees, but also to anyone who has applied, or will apply, for a vacancy at your organisation.

We are upgrading CIPHR iRecruit so that it can be configured to meet the requirements you have determined are necessary for your recruitment processes to comply with the GDPR. If you are not currently using an applicant tracking system (ATS) for recruitment, or are using another ATS, be sure to check that your processes will be GDPR compliant from 25 May 2018. Please contact your account manager if you aren’t currently using CIPHR iRecruit and would like to arrange a demo.

Changes for applicants

How applicants can consent to data processing

If you have determined that you need to gain consent from a candidate in order to process a job application, CIPHR iRecruit can be configured to seek this consent. If this configuration is turned on, when candidates submit applications or register for an account on your application portal they will be asked to consent to the collection and processing of their personal data, and to agree to the site’s terms and conditions. If they do not give consent, or agree to the terms and conditions, they will not be able to register for the site or submit an application.

CIPHR iRecruit will feature a standard data privacy statement created by CIPHR, but your organisation should also create and upload its own data protection consent statements that reflect how you will use the data, and how long you will retain it for.
GDPR compliance

Figure 3: example of privacy policies shown to candidates when submitting applications through CIPHR iRecruit. The configurable organisation-specific policy is shown in yellow. The text in the grey area is CIPHR’s standard privacy policy but can be configured.
How applicants can withdraw or extend consent

If you require consent from job applicants to hold and process their data, applicants can withdraw or extend their consent at any time via the candidate portal.

If you have required candidates to give their consent to the collection and processing of data through CIPHR iRecruit, they will be able to remove or extend their consent at any time using these options in the candidate portal.

If you have configured CIPHR iRecruit to seek consent from an applicant and currently do not have their consent, CIPHR iRecruit will not allow you to ‘process’ the candidate’s data, ie you will not legally be able to contact them. Their details will also be highlighted in a dashboard as requiring deletion, which you can do either individually or in bulk.

How applicants can request access to their data

Applicants can request a download of their personal data from the system via the candidate portal. An HR administrator will need to approve the request, and then a button will become available in the portal, enabling the candidate to download their data.
Figure 5: if a candidate has requested access to the data held about them in CIPHR iRecruit, and an HR administrator has approved the request, the candidate will see a 'download' option in the candidate portal.
Changes for HR administrators, recruiters, and managers

If you have configured CIPHR iRecruit to seek consent from an applicant, you will be prevented from contacting candidates if their consent has not been given, has been withdrawn, or has expired.

Alternatively, if you are not relying on consent to process the personal details of job applicants, you can configure a data-retention period that is in line with your published privacy statement. When the specified retention period for a candidate has lapsed, CIPHR iRecruit will prevent you from contacting them.

A new data protection dashboard indicates each record’s retention period (it is up to you to define the appropriate retention period), as well as giving you the ability to:

- Download the candidate’s data
- Enable the applicant to download their own data via the portal
- Ask the candidate to extend their consent if required
- Anonymise the candidate’s record (ie delete pre-defined sensitive data fields, while retaining all non-sensitive fields, enabling you to report on the record as part of your HR reporting)
- Delete the record entirely

You can perform all these functions either for individual records, or in bulk.

Figure 6: example of the data protection dashboard in a CIPHR iRecruit system that has been configured to seek consent from applicants, showing the status of different candidate records and offering options to grant access to data download requests, request consent extension, anonymise data, and delete data
CIPHR iRecruit will also flag in the recruiter profile if the data-retention period for a candidate's records has lapsed, and the recruiter will not be able to make contact with the candidate.

![Figure 7: recruiter profile in CIPHR iRecruit, showing the data retention period for this candidate has lapsed](image)

**Important points to note about using CIPHR iRecruit under GDPR**

- You must determine and define the data retention period. This period will be the same across all vacancies and for all applicants
- If you have configured CIPHR iRecruit to seek consent from candidates to process their data, they will not be alerted when their consent is about to expire. HR administrators must actively log into the system and request that the candidate extends their consent. If you are not seeking consent, and are keeping data based on data retention periods, again, the candidate will not be alerted when this period has lapsed
- When the retention period you have set expires, you have 30 days to take action (ie to request the candidate's consent for an extension, anonymise the record, or delete the record). Records will not be deleted automatically; it is your responsibility to take action
- This 30-day grace period will apply to candidate records in CIPHR iRecruit on and after 25 May 2018, so be prepared to take action after that date or risk losing the ability to contact candidates. There may be hundreds or thousands of records that require your attention
• If you have configured CIPHR to seek consent from candidates to process their data, consent withdrawal or expiration does not lead to the automatic deletion of data; it means you are not legally able to contact the candidate to request their consent

If you have any questions about using CIPHR iRecruit to comply with the GDPR, contact the service desk.

If you currently don’t use CIPHR iRecruit to manage your recruitment processes and would like further information, call us on 01628 814 060, email cm@ciphr.com, or contact your account manager.

Understanding GDPR

We would strongly recommend that you seek your own legal advice if you are unsure about the implications of the new data protection laws on your business.

Legal disclaimer

The information contained within this document is for general guidance purposes only. It should not be taken for, nor is it intended as, legal advice. While we have made every effort to ensure that the information provided on this document is correct and up to date, CIPHR makes no promises as to completeness or accuracy and the information is delivered on an “as is” basis without any warranties, express or implied. CIPHR will not accept any liability for errors or omissions and will not be liable for any damage (including, without limitation, damage for loss of business or loss of profits) arising in contract, tort or otherwise from the use of or reliance on this information, or from any action or decisions taken as a result of using this information.
Get in touch

Abbey House
28-30 Chapel St
Marlow, Bucks
SL7 1DD

01628 814 060
cm@ciphr.com

ciphr.com
@ciphrhrsoftware
ciphr