Employee/Candidate Data Privacy Notice

Version Number	**6.0**
Next Review Date	**22 March 2026**

Contents

General

This document outlines Cabot Financial (Ireland) Limited ("Cabot", "Us", "We", "Our") approach to Data Privacy and how we fulfil our obligations under the General Data Protection Acts 1998 to 2018 and the General Data Protection Regulation 2018 ("GDPR") in respect of Cabot employee personal data. We take our obligations very seriously when dealing with your personal data. We have outlined throughout this Employee Data Privacy Notice the way in which we carry out our obligations.

Cabot is part of the Cabot Credit Management Group and Encore Capital Group (together "Group").

Personal data means data relating to a living individual who can be identified (either from that data itself or when combined with other data).

Our Privacy Promise to you

- We promise to be fair and transparent in all our dealings with you
- We treat the security of our colleagues and contractors' personal data very seriously
- We believe in integrity, but above all, we will always respect your privacy in relation to your personal data.

Our Employee Data Privacy Notice provides you with information about how we use your personal data. Please use the list below to choose which section of our Employee Data Privacy Notice is most suitable for you:

- What type of personal data we collect?
- How do we collect your personal data?
- How we use your personal data?
- How long do we retain your personal data for?
- Who we share your personal data with?
- Transferring your personal Data outside of the European Economic Area
- How we keep your personal data safe?
- Your rights in relation to your personal data
- Who can you speak to about this Privacy Notice?

What types of personal data do we collect?

The types of personal data that we collect may include, but is not limited to, the following:

- Contact data/identity data: Including name, proof of identification, date of birth, address, gender, nationality, marital status, telephone number, email address, emergency contact information and photograph
- Details about your previous employment/current employment: Including employer name, length of service, business titles, details of your role(s) and references
- Qualifications: Including skills, education, continuous professional development ('CPD') compliance (if applicable), the languages you speak, your eligibility to work in a particular country, interview notes and your work experience

- Publicly available information: Including details we gather from publicly available sources where such sources are relevant to your job
- General employment records: Including details of training, disciplinary and grievance matters, benefits, holiday and other absences, employment contract, performance records (including appraisals), salary history, settlement agreement terms
- Information gathered through monitoring of IT systems, building access records, and CCTV recording
- Financial details: Including information provided to facilitate payroll
- Information from Employee Satisfaction Surveys where not anonymised
- Information in relation to data access, correction, restriction, deletion, porting requests and complaints
- Information through companies which we use to validate for financial crime purposes
- Special categories or sensitive personal data: Some categories of personal data are more sensitive than others. These are known as special category personal data which include:
    - Racial or Ethnic origin;
    - Biometric data;
    - Religious beliefs;
    - Data concerning health
    - Data concerning sexual orientation

If you ever disclose special category personal data to us (such as disability data, medical history details or health related data), we will only keep this on record if it is necessary for the relationship between both parties. Where we do need to keep this data, we will always request your explicit consent to do so. We will only store this data for as long as it is relevant.

You have the right to withdraw your consent and if you do, we will delete the special category data from our records, where appropriate. If you disclose special category personal data to us without us having the opportunity to obtain explicit consent, for example, sending a letter or email to us detailing your medical situation, you will have given your consent for us to process that data. Where we consider it necessary to record the special category personal data you give to us, we will securely record this information and tell you in writing how we will use it and how you can withdraw your consent.

How do we collect your personal data?

We collect your personal data in the following ways:

- We will make a request to obtain your personal data from you
- You voluntarily submit your personal data
- We obtain personal data from third-party data sources including recruiters, previous employers, providers in relation to employment/ongoing checks such as financial sanction checks (Cabot utilises a third-party screening tool) or publicly available information, or where you are referred to an open position by an employee as part of a Cabot referral program

- We keep records of correspondence between us, which may include letters, live chat, email, SMS, and social media communications. Also, communications through Cabot devices
- We operate CCTV at our business premises, so on attending our office your image may be captured on our CCTV
- Third parties that we appoint may collect personal data from you and pass it on to us. This could include our payroll which is outsourced to a third party
- We collect data provided as part of Employee Satisfaction Surveys, where not anonymised
- We collect data concerning your access to our building, usage of our business emails and website facilities.

How we use your personal data?

We collect and process your personal data for a variety of reasons, including:

- To meet our contractual obligations to you
- To manage the performance of the contract we have with you
- To assess your suitability for positions within our organisation
- To manage our operations and continuously improve our service
- To manage security, risk, and crime prevention
- To meet our regulatory requirements
- To undertake statistical analysis for business improvements

To process your personal data, we need to have a legal basis for doing so. Put simply, this means that processing your personal data must be necessary for one or more of the following reasons:

- To comply with a legal or regulatory obligation
- Where we have a legitimate interest
- To perform a contract that you are party to
- When you give us your consent or
- To protect your vital interests

The table below sets out different scenarios of our lawful basis in which we may need to process your personal data. This list is not exhaustive, and we may undertake additional processing of personal data in line with the purposes as set out above.

Business Process	Our lawful basis for processing	How do we use your data?
Recruitment	• Legitimate interests • Compliance with a legal or regulatory obligation • Where you give us your consent	CFI collects personal details about you as an individual, your career, competence history and your qualifications. As part of this process, we would need to perform checks on the above to validate this information you have given us
Management of your Contract	• Compliance with a legal or regulatory obligation • Legitimate interests	As a business, we have an obligation to manage your contract in accordance with our agreement. We provide you with statutory

	• To perform a contract	communications and payments and use your data to comply with health and safety requirements in association with your contract. We have a legitimate interest in ensuring your safety and wellbeing at work and therefore process data about your medical history which may affect performance in your role. We process your data to administer benefits under your employment contract and to administer annual leave or other leave.
Train, Monitor and Improve our service	• Compliance with a legal or regulatory obligation • Legitimate interests • Performance of a contract	We use recordings of transactions and refer to competence and career development history to train our employees and monitor diversity. We use your data to consider eligibility for a promotion or for alternative roles and to manage performance, including appraisals. We use your data to conduct ongoing training modules internally and externally to meet our regulatory obligations and to provide ongoing training relevant to the company. We may choose to ask another company to contact you to request feedback which would enable us to make improvements where necessary (such as employee surveys). We monitor your website usage, collecting data from your usage to improve our business efficiencies and statistical and analytical activities and to monitor the proper use of Cabot's IT systems
Comply with Legal and Regulatory Requirements	• Legitimate interests • Performance of a contract • Compliance with a legal or regulatory obligation	At times we share data with other third parties where we have a legal or regulatory requirement to do so. For example, we may share your data with the Central Bank of Ireland as part of fitness and probity/minimum competency code.
Address disciplinary and grievance issues	• Legitimate interests • Performance of a contract	We use your data to keep a record of discussions and any formal action taken.

How long do we retain your personal data?

Your personal data is retained for different periods of time depending on the purposes for which it is required to be retained. We will keep your personal data on file for as long as you are an employee or contractor of Cabot or the group. Please refer to the table below which details all relevant data retention periods for different categories of data.

Documents	Retention Period **(add one additional year)
Personal Data e.g., Photo ID & Next of Kin Information	**Personal data shall not be kept for longer than is required by the relevant statutory provision** – Deleted at leaving agreement termination date
Employment Agreement – Contract related / terms of employment	**7 years** from end of employment
Employment Agreement of Directors – Contract related / terms of employment	**7 years** from end of employment
Employee Benefit Plans (insurance, pension, retirement etc.)	**Indefinitely**
Contributions/Distributions	**7 years** from end of employment
Elections and Promotions	**7 years**
Interviews and Employee Selection	**1 year**
Job Descriptions	**1 year**
Evaluation Records	**7 years** from end of employment
Personnel Files & Employee Records	**7 years** from end of employment
Permit Records	**5 years or for the duration of the employment** (whichever is the longer)
Medical Records	**7 years** from end of employment
Accidents / Injury Reporting	**10 years** from date of an incident
Workers' Compensation Claims Personal Injuries (including fatal injuries)	**7 years** from end of employment
Actions based on tort or contract	**7 years** from end of employment
Health & Safety	**7 years**
Parental Leave and Force Majeure Leave	**12 years**
Carer's Leave	**8 years**
House of work, annual leave, sick leave and public holidays	**3 years**
Training/ Development	**7 years**
Salary (Administration Only - Payroll data retention requirements above under Finance/Tax)	**7 years**
Taxation Records	**6 years**
Collective Redundancies	**3 years**

Please note that in certain circumstances, we may hold your personal data for a longer period, for example, if we are processing an ongoing claim, defending litigation, or believe in good faith that the law or a relevant regulator may reasonably in our view expect or require us to preserve your personal data. When personal data reaches its maximum retention period, we will ensure that this data is purged from all systems including filing systems and storage units, etc. We will then destroy any hard copies of personal data we may hold using our confidential waste disposal providers.

Who we will share your data with?

We only share your personal data with a select number of individuals and companies and only as necessary. Sharing can occur in the following circumstances and/or with the following persons:

- Staff in Cabot: We may share your personal data with individuals/business units within Cabot such as HR, IT, Finance/Payroll, Managers, System Administrators and/or Risk & Compliance
- Staff/Companies in Group: We may share your personal data with other staff/companies within Group, for example, if we instruct another company within the Group to act on our behalf or perform administrative duties, or for HR purposes
- Third parties: We may share your data with third parties who assist us with recruitment, campaigns, and/or ongoing screening such as recruitment agencies, background check companies, financial crime screening companies, etc.
- Previous employer – We may share your data with your previous employers when you have provided them as a reference and/or third parties that may be contacted to provide additional information related to your previous work experiences
- Suppliers and service providers: For example, companies that provide us with IT or cloud services, infrastructure, payroll, benefits facilitation, training and development and/or mailing service
- Your bank for the payment and processing of payroll
- Regulatory authorities
- Professional advisors such as legal advisors, consultants, and accountants.

It is possible that we may also need to disclose personal data about you when required by law, or if we have a belief that disclosure is reasonably necessary in the following circumstances:

- To investigate, prevent, or act regarding suspected or actual illegal activities or to assist government enforcement agencies
- To enforce our agreements with you
- To investigate and defend ourselves against any third-party claims or allegations
- To protect the security or integrity of our Service; or
- To exercise and/or protect the rights and safety of colleagues, contractors, or others.

We will share your personal data if our business was sold to another company, but it must continue to be used in accordance with this Employee Data Privacy notice. We can also share your personal data as part of any merger or change in control of the business, or in preparation for any of these events. Any other entity which buys our business or part of the business will have the right to continue to use your personal data

Sharing your personal data for the prevention of crime or harm

We have systems that protect our customers and our business against fraud and other financial crimes including money laundering and terrorist financing. Employee personal data can be used in two ways, either to prevent a financial crime and/or trace those responsible for committing a financial crime.

If fraud or any other financial crime is suspected, or has been identified by Cabot, we are also obliged to pass your personal data to fraud prevention agencies or other authorities in the state working towards the prevention and/or detection of financial crime in Ireland. The Company, under law, has legal obligations to pass this data to fraud prevention agencies. This will be our legal basis for sharing your personal data in this way.

The agencies we may need to share your personal data with are:

- An Garda Siochana
- The Revenue Commissioners
- The Anti-Money Laundering Compliance Unit,
- Dept. Justice and Equality
- Any other Fraud Prevention Agencies within the state

Transferring your personal data outside of the European Economic area (EEA)

We may transfer your personal data to our service providers (such as IT service providers) and individuals/companies within Group that operate outside of the European Economic Area (EEA) (for example for HR purposes). Where we authorise the processing/transfer of your personal data outside of the EEA, we require your personal data to be protected and include one of the following data protection transfer mechanisms:

- Model Clauses (also known as Standard Contractual Clauses) are standard clauses in our contracts with our service providers and other organisations
- Transfers to countries outside the EEA which have adequate level of protection as approved by the European Commission
- Binding Corporate Rules
- Transfers permitted in specific situations where a derogation applies as set out in Article 49 of the GDPR.

How we keep your personal data safe

We know that you care about how your personal data is used, stored and shared. We appreciate your trust in us to do that. To protect your personal data, we use security measures that comply with Irish Law and meet international standards. This includes computer safeguards and secure files.

Your rights in relation to your personal data

You have a number of rights in relation to the personal data which we hold about you. If you choose to exercise any of these rights, we may ask you to verify your identity by providing us with additional information, such as up to date proof of identity or address.

Right to object:

You have the right to object to us processing your personal data if the processing itself is an unwarranted interference with your interests or rights.

Right to restrict processing:

If you believe we are processing your personal data unlawfully, or if you believe that we no longer need your personal data, you have the right to request that we restrict the processing of your personal data.

Right to Erasure (Right to be forgotten):

You have the right to request that we delete your personal data if you believe we no longer have a lawful basis to process it, provided there are no legal obligations or overriding legitimate grounds that require us to keep it.

Right to rectification (correct your personal data):

Upon obtaining your personal data we conduct checks to validate that it is accurate and up to date. We are reliant on you and other third parties to provide us with the correct personal data at all times. If you believe that any of the personal data we hold for you is incorrect, it is important that you make us aware of this as soon as it is possible, for example if you have a new phone number or you have moved address you will need to update us with your new contact details.

Right to make a complaint to the Data Protection Commission:

You have the right to make a complaint to the Data Protection Commission ("DPC") if you are not satisfied with the outcome of your complaint with us. You can contact the Office of the Data Protection Commission at:

- **Website:** www.dataprotection.ie
- **Telephone:** +353 (0)7650100 / 1800437737
- **Email:** info@dataprotection.ie
- **Writing:** Data Protection Commission, 21 Fitzwilliam Square South Dublin, D02 RD28

Right to withdraw your consent:

For certain limited uses of your personal data, we may ask for your consent. Where we do this, you have the right to withdraw your consent to further use of your personal data where the processing is based on your consent. If you withdraw your consent, it will not affect the lawfulness of processing based on your consent before its withdrawal.

Right to portability:

You can request that certain personal data which you have provided to us be transferred to you or to another service provider.

Right to access your personal data:

You have the right to get confirmation about whether we process any of your personal data and, if so, how we use it. We use this Employee Data Privacy Notice to meet this obligation. In addition, if we process your personal data, you have a right to request a copy of the personal data that we process.

In order to make this request, please contact us on the below details:

- **Writing:** HR Team, Cabot Financial Ireland, PO Box 11151, Tallaght, Dublin 24
- **Email:** HR@cabotfinancial.ie
- **Telephone:** 01-4649000

Right to object to a decision based solely on automated processing:

You have the right to object to a decision based solely on automated processing, where such processing produces legal effects or significantly affects you.

Who can I speak to about this Privacy Notice?

If you would like to make a complaint or have a query about how we use your personal data, you can contact us at:

- **Writing:** Data Protection Officer, Cabot Financial Ireland, PO Box 11151, Tallaght, Dublin 24
- **Email:** dataprotection@cabotfinancial.ie
- **Telephone:** 01-4649000

OR

- **Writing:** HR Team, Cabot Financial Ireland, PO Box 11151, Tallaght, Dublin 24
- **Email:** HR@cabotfinancial.ie
- **Telephone:** 01-4649000

If you are unsatisfied about how we have handled your complaint, you have the right to escalate your complaint to the DPC. You can contact the DPC at the contact details provided above.