First Central
Insurance & Technology Group

First Central - Privacy Notice

First Central
Insurance & Technology Group

Contents

Welcome to First Central

This is our full privacy notice and tells you how we collect and use personal data for:

- **Candidates and Applicants**
- **All Current Employees** including contractors, agency workers, consultants, directors and associated third parties; such as your emergency contacts and next of kin.
- **All Former Employees**

About this notice

The notice is provided on behalf of all the First Central Group of companies that operate across the United Kingdom, Guernsey and Gibraltar providing insurance and technology services (hereafter "**First Central**"). It will describe our processing activities, our legal grounds for the activity, sharing of personal data, your rights, how long we will retain your information and how we will secure it. We are obligated to comply with the General Data Protection Regulation (GDPR) and the Data Protection Acts of Guernsey, Gibraltar and the UK.

We understand the legal responsibilities we have to protect the information you provide us at any stage of your engagement with us, and will only use the personal data provided for the activities we have identified.

If we are required to perform a new activity that is not compatible with our original reasons for collecting the information, we will provide additional information to you about that activity.

We may need to seek your consent to perform certain activities. If consent is needed, we will engage this with you separately so that we can be sure consent is freely given, informed and explicit. Please note that we do not need to obtain your consent for every activity we perform.

The First Central Group company identified in your application or employment contract (or subsequent contract change documentation) will be the controller of your personal data and special personal data. It is important that you consider this notice in conjunction with your employment contract, where applicable.

There are a set of key definitions available at the end of this notice to help you.

Contact

If you have any questions or concerns about this notice or want to exercise any of your rights, you are invited to contact our HR team at Human.Resources@first-central.com, Recruitment at Recruitment@first-central.com or the Group Data Protection Officer at DPO@first-central.com.

Updates

We may amend this notice from time to time to keep it up to date with current legal requirements and the way we perform our activities.

General Information

We are obligated to ensure that for each activity we undertake with your personal data, we have identified what lawful reason we have to perform that activity. If the activity requires us to use special personal data**,** we will also consider a secondary ground to perform the activity.

The following legal grounds are the ones we most commonly rely on:

Legal grounds for activity with Personal Data	**Description**
The **activity** is necessary for **entering into or performing a contract**	The personal data is needed for performing the contract to which you are a party, or in order to take steps at your request prior to entering into such a contract. For example, we need information to be able to pay you or provide you with contracted benefits.
The **activity** is necessary for us to meet **legal obligations**	When we need to comply with the law we will need to use information about you. For example, to ensure we meet tax requirements.
The activity is needed for our **legitimate interest**	The activity may be one that is necessary for our or a third party's legitimate interest. Where we are relying on this ground as the basis for the activity, we will tell you what our legitimate interests are in this notice. We can carry out any actions we consider are needed for these interests as long as we consider that the activity does not negatively infringe on your privacy rights and interests.
Legal grounds for activity with Special Personal Data	**Description**
The **activity** is necessary for complying with the **employment law obligations**	The personal data is used to carry out the obligations and exercising the rights of you or us in the field of employment law, social security and social protection law. This means that we can carry out any actions we need to undertake in order to comply with obligations under employment law or for health and safety.
The **activity** is necessary for a **substantial public interest**	This includes activities for the purposes of preventing or detecting unlawful acts, equality of opportunity or treatment between different groups of people and as a result of regulatory requirements relating to unlawful acts and dishonesty. These interests are defined in the law.
The **activity** is necessary for **insurance purposes**	If we need to set up or have insurance in place for you, we will use personal data in the application process.
The **activity** is necessary for **legal claims**	If we are pursuing or defending a legal claim, we may need to use personal data as part of the claim.

Sources of personal data

There are four ways that we will collect personal data about you:

From you directly

We will ask you to directly provide us with your personal data. This will be at the point of recruitment when your journey starts with us. The personal data will be collected through our website and through the CV and covering letter that is provided. During the course of employment, you may provide additional personal or special personal data.

Internally

Over the course of your journey with us, personal data will be created about you. This is usually generated through your Line Managers, for example, in your appraisal records or interview records. Personal data may be collected indirectly from monitoring devices such as from CCTV, building and location monitoring systems, telephone logs, and recordings and email and Internet access logs.

Externally

We will need to collect some personal data about you from third parties such as previous employers, through background vetting, benefit providers or medical providers. It is not possible to list all the third parties in the notice, as they may vary depending on your role or location.

Publicly

We may also obtain information from publicly available sources such Government or Regulatory platforms or social media channels were applicable.

Sharing your information

As you move through the stages of your journey with us, we will need to share your personal or special personal data with third parties. Sharing activity is detailed as you progress through the notice.

If the third party is a Controller, we will provide details about where you can find and read their notices. If the third party is a Processor, we will only share your personal data with them to the extent necessary for them to carry out the tasks they are performing on our behalf i.e. carrying out background screening through our selected provider.

At First Central, your personal data is accessible on a least access basis e.g. by HR or by your Line Manager and will only be shared with other companies in the group for reporting purposes where necessary.

Candidates and applicants

When you apply for a role at First Central, we perform certain activities to manage and administer your application:

Activity	Details
Accepting your application	We need to identify you and contact you in order to proceed with your application. All communications will come from our Recruitment team or the Hiring Manager. We will use your contact details, eligibility to work in the UK and identity information to accept your initial application. We do this on the basis of yours and our legitimate interest to start the recruitment process and to meet our legal and regulatory obligations. We do not add any additional information to your application at this stage. The personal data we collect: - Name - Contract details - Address - Your CV - Financial status* - Right to work* - Criminal records* * These questions require a yes/no answer only at this point in the journey. If your application is received from a recruitment agency or other third party, this information will be received by them and shared with us. Check their privacy notices.
Setting up the interview	If your application is successful, we will contact you to set up an interview. At this point, we will ask for additional information such as any relevant health information in order that we can make reasonable adjustments. We do this to ensure we can meet our legal obligations under social protection laws such as the Equality Act.
Diversity and equal opportunity monitoring	We collate data regarding your ethnicity, gender and age for the purposes of monitoring equal opportunities and diversity in the workplace. This information will become anonymised on conclusion of your application. We do this on the basis of performing equal opportunity monitoring.
Assessment and selection	To assess your suitability for the role, we will use your personal data, specifically the contents of your CV e.g. employment history, educational history, qualifications and personal achievements and skills, to consider you against other candidates and against our role specification and needs.

	We may add additional information to your application as you proceed through the selection process from the activity, such as from you, our managers and recruiters. We may also consider regulatory information if the role you are applying for is a role regulated by an applicable financial services authority. We do this in our legitimate interest to recruit the right candidate for the company. In addition, for regulated roles we will also process the data on the basis of legitimate interest in complying with our regulatory obligations.
Making an offer / onboarding	If you make a successful application, we will use your personal data to make that offer to you and to produce the appropriate documentation. This will also start our process for background screening. We will use your identity information, contact details, skills information and regulatory information. If you accept the role, we will also collect your payroll information. We do this on the basis of taking steps to enter into a contract with you and in our legitimate interest to onboard you to the company.
Background screening	If we make an offer of a role, we are required to conduct pre-employment vetting and background checks on your financial status, employment history and professional qualifications. We have a selected provider who supports us in this process. They will contact you by email to start the process. We will do this on the basis of entering into a contract with you and our legitimate interest in meeting our regulatory obligations and protecting our business. We will also receive confidential references from former employers and other such referees as you provide.
Regulated roles – additional steps	If you have applied for a role that is subject to regulatory requirements set out by the FCA, we will need to perform additional activities within the background screening. This will include an assessment of your fitness and propriety to perform the function and your regulatory status. We will also need to obtain regulatory references. We will do this on the basis of entering into a contract with you and our legitimate interest in meeting our regulatory obligations and protecting our business.
Criminal record screening	Our selected provider will also support us in conducting a criminal record screening with the Criminal Record Bureau. The screening is only performed once an offer of a role has been made. We do not receive the output, this will be sent to you directly, however, we are advised if there is anything to note on the report.

	We do this on the basis of entering into a contract with you and our legitimate interest in meeting regulatory obligations and protecting our business.
Right to work	We are legally required to ensure that all successful applicants have the right to work in the UK prior to them starting with us. If we are supporting you to obtain a visa, or to make any other such application, we may collect additional information from you, such as the date you came to the UK. We will do this on the basis of meeting our legal obligations.
Your next of kin	If you accept the role, we will ask for information about your next of kin. We collect this information for emergency purposes. We will store their name, relationship to you and their contact number. In the event of an accident or emergency, we will contact them. We recommend that you confirm to your next of kin that we will store this information. We will do this on the basis of yours and our legitimate interest in the event of an emergency. If we have to share this information with the emergency services, it will be because there is a vital interest.
Reporting	We monitor the success of our campaigns and monitor our recruitment process. The personal data may be used to assist us in our reporting. This helps us drive better business decisions regarding our resourcing and business structure. Where possible, this will be done using anonymised information. We will do this on the basis of our legitimate interest to understand and analyse our business.

All the information captured during the application process will be stored within SelectHR or as a physical record. This information will only be accessible by our HR team and by your Line Manager. We do not share information of applicants with any external third parties unless they are successful following the interview stage.

Unsuccessful applications are retained for a period of 12 months, unless we are required to retain the information in accordance with the law or we require an accurate record of our dealings in the event of complaints or challenges, or if we reasonably believe there is a prospect of litigation.

If you are successful in your application, we will share your personal data with the following third parties as part of our onboarding to the company. This list is not exhaustive:

Background screening provider	Tax authorities	Life assurance provider
Payroll provider	Pension provider	First Central Group of companies for setting up IT services

All current employees

Now you are an employee of First Central, we will perform activities with your personal data to manage your employment and give you access to our benefits.

Activity	Details
Employee management	During the course of your employment, we will perform activities that allow us to administer your employment contract. This will include ensuring: • the information we hold is kept up to date • we can handle employment queries • we share data with applicable authorities • the performance of any other management activity that is a part of our employment relationship with you We will perform these activities on the basis of **performance of the contract** and to meet our **legal obligations**. If these activities require us to use medical information in the performance of your contract, this will be done on the basis of carrying out **employment law obligations**. If these activities include criminal data through ongoing or retrospective screening, we will perform these activities for **the prevention and detection of fraud** and in our **legitimate interest in meeting our regulatory obligations**. Data may be generated by third parties, such as occupational health or through monitoring services, and they will be made available to you. All documentation updates will be stored in SelectHR and you can access this at any time during your employment. We will ask annually that you check your personal data for completeness and accuracy.
Payroll and tax administration	We will process your personal data to ensure that the terms of your employment contract are being met in relation to your pay. We will also use your information to ensure we meet our obligations in respect of tax administration, such as issuing P45s, P60s, expenses etc. We may receive and share information from third parties to manage this activity, such as the court service or local tax authorities. We will do this on the basis of **performing the contract** and to meet our **legal obligations**.

Pension administration	You are legally entitled to be auto-enrolled into our Pension Scheme and this is something we offer under your employment contract. We will share your personal data with our pension administration company and you will receive your own access to manage and monitor this. We will do on the basis of **performing the contract** with you and to meet our **legal obligations** in respect of auto-enrolment.
Absence management	We use your personal data and information collected from your Line Manager to manage any absence. This can include holiday, sickness, compassionate and all other statutory types of leave. All absence is recorded on our central HR system. We will do this on the basis of **performing the contract** and to meet our **legal obligations**. If these activities require us to use or collect additional medical information in the performance of your contract, this will be done on the basis of carrying out **employment law obligations**.
Learning and development	During the employee journey, we actively encourage and support learning and development in your role, as it benefits not only us but you. We will therefore use your personal data to ensure that you can receive training internally or externally. Information about your learning and development will be stored in our learning system, which you have access to. There may be external providers that require to you to agree to their privacy notices. In such cases we will make these available to you at the outset. We may need to share personal data with external providers and may receive some personal data, such as the completion status in return. We will do this activity in our **legitimate interest to ensure our employees can receive necessary training and development for their roles**.
Managing our talent	We monitor the performance of our employees to ensure we can manage talent effectively. We will use personal data to do this, such as your performance records. Performance records like appraisals and feedback are available for employees to access on our Perform system. We will do this activity in our **legitimate interest in ensuring we manage our talent effectively**.

Restructure, transformation or reorganisation	We do, on occasion, have to reorganise, transform or restructure our company to support its long-term objectives and growth. In order to do this effectively, we have to use personal data – specifically job information or performance information, remuneration information, skills and talent management information. We may instruct third party consultants to support us in this, which will require sharing information with them. We will do this activity in our **legitimate interest in ensuring our company is managed effectively** and to comply with our **legal obligations**.
Employee benefits	We offer a wide range of employee benefits in addition to those you are entitled to under your employment contract, such as: • Recommend a friend • Central Perks • Discounts on car insurance • Cycle to work • Easit membership • Metrolink discount • Employee Assistance Programme • Give as you earn • Holiday Extra • Health insurance schemes • Local discounts • Professional subscriptions • Season ticket loans • Volunteering All of these benefits are extras we can provide, and therefore, you can choose if you want to use them. When you choose to use a benefit, we will need to process your personal data to provide the services; this will include sharing your personal data with the relevant third party benefit provider. It is not always possible to obtain your consent for sharing data with the providers of these benefits, therefore, we will do this on the basis of **legitimate interest of providing benefits to our employees**. We will, however, only ever share what is required for the provider to offer you the benefit.

Rewards	We offer our employees rewards for continued service, for milestones in their journey with us, for performance through “Leading the Way” or “Red Letter Days” as well providing opportunities to bring the company together, for events like the anniversary or summer parties. We will need to use your personal data to provide access to the rewards platforms and for the administration of events. We recommend you review the privacy notices of the rewards platforms for more information on how they will use your personal data. We will do these activities for our **legitimate interest in providing our employees with access to rewards.** We will limit what personal data we use for these purposes to what is necessary.
Employee engagement	There are two elements of how we may process your personal data for engagement with us: 1. Communication – we will provide business updates, offsite days and changes to working practice notifications. We rely on a number of tools to communicate with our employees. We primarily direct communications to your work email, however, if you are on leave for whatever reason, we may send such communication to your personal contact addresses. Our communication tools rely on us providing work emails to set up accounts and create communication channels. 2. Employee surveys – we conduct employee engagement surveys at least annually and other surveys where we want your feedback. You will have an option about what information you provide in these surveys and responding is completely voluntary. We may combine data received with other surveys, historic surveys or with other employee data factors like role and department. These surveys are used for research and analysis and to make improvements. We carry out these activities on the basis of **legitimate interest for employee engagement, assessing satisfaction levels or to make improvements to our working practices**. We may engage third parties to support us in collating and producing surveys and will share personal data for this purpose. We limit what personal data is shared for this purpose.

Legal and regulatory compliance	As a legally established and regulated group of companies, we have legal and regulatory obligations that we have to comply with, which require us using your personal data. Examples of these legal obligations: • **Health and safety** – maintaining accident log books and visual display assessments or personal evacuation plans, or homeworking assessments • **Working time or practice regulations** – maintaining policies or appropriate contracts • **Tax authorities** – providing end-of-year financial reporting or other disclosures • **Obligations imposed by the FCA, PRA or another regulator depending on the jurisdiction** – reporting on working practices • **Occupational health** – for making reasonable adjustments to working conditions or providing health services • **Law enforcement or public authority** – request if applicable • **Legal advisors or courts** – requests for disclosure or engagement in proceedings Where such an activity requires special data to be shared, this will be done on the basis of carrying out our **employment law obligations**. There activities will be done on the basis of meeting our **legal obligations** or in our **legitimate interests in meeting our regulatory obligations**.
Investigations and protecting the company	We perform activities which are for the protection of you and our company. These activities include monitoring the behaviour, conduct and activities of our employees. If we receive rereferrals that require investigation, this will be done by appropriate employee levels in the company. We will do this through our systems and records and may need to complete retrospective screening. In certain circumstances the personal data may be collected through indirect means, such as access control logs and monitoring systems, telephone logs, CCTV and internet access logs. These activities will be done on the basis of our **legitimate interest in protecting you, our customers and our company, and in meeting our regulatory obligations**. If special personal data is involved, this will be done under a **substantial public interest reason, such as prevention and detection of crime or fraud**.

Complaints, disciplinary and grievance management	Our HR team is responsible for investigating complaints, disciplinaries or grievances raised by our employees. They will process your personal data to do this, which may require the collection of additional information from third parties, whether internally or externally sourced, as part of the investigation process. Our procedures for management in these areas are detailed in our internal policies. We also follow ACAS guidance in our management of this. This is done on the basis of meeting our **legal obligations**. This may include special personal data, including health information or criminal screening information. This activity will be done on the basis of **meeting our employment obligations** and for **substantial public interest reasons**.
Reporting (generic)	We will use the personal data to analyse trends and patterns, such as department performance in order to make better business decisions, or to monitor absence for resourcing needs. Depending on the subject of the analysis, we will limit the personal data used to what is necessary to produce our reports. We do this in our **legitimate interests to ensure that our business is running effectively and to understand our business operations**.
Managing your departure / Offboarding	If you make the decision to leave the company, we will start the process of offboarding you and to manage your departure. This will include an exit interview. We will do this on the basis of **performance of the contract** and in our **legitimate interest to ensure the appropriate termination of the relationship**.

All former employees

If you leave us, your personal data will then be used in very limited circumstances. This is primarily the group retaining a copy of the personal data and what comprises that for the retention period. We do this in our **legitimate interest to ensure we can provide employment references if needed, manage any complaint or possible employment claim, or to comply with our legal obligations**.

Information about third parties

We use third parties to support some of the above activities. Here is a list of Controllers with links to their applicable privacy notices for your reference:

Company	Link
Central Perks	https://centralperks.fizzbenefits.com/TermsAndConditions
Easit	https://www.easit.org.uk/storage/user/easit%20privacy.pdf
Give as you earn	https://www.cafonline.org/privacy
Simply Health cash plan	https://www.simplyhealth.co.uk/about-us/privacy
Pension provider Also refer to policy documents	The People's Pension - https://thepeoplespension.co.uk/privacy/ Aegon - https://www.aegon.co.uk/support/faq/privacy.html Blue Riband - https://pensions.bwcigroup.com/privacy-policy/ Gibraltar State - https://www.gibraltar.gov.gi/privacy-policy
Life Assurance	https://www.omnilife.co.uk/privacy-policy/
Private Medical Cover Also refer to policy documents	Bupa - https://bupa3.xexec.com/Pages/Privacy Axa - https://www.axa.co.uk/privacy-policy/ Now Health - https://www.now-health.com/gb-en/privacy-policy/
Long Service Awards	https://www.aspirationsonline.com/privacy-policy.asp
Red Letter Days	https://www.redletterdays.co.uk/privacy
Occupational health	https://www.sherrardslaw.com/privacy/
Employee assistance	https://www.healthassured.org/privacy-policy/
Chartered Insurance Institute	https://www.cii.co.uk/about-us/data-protection-and-privacy-statement/

It is not possible for us to provide the details of every Controller we may share your information with as part of undertaking these activities, as it could be a specific third party to a particular employee, depending on the activity e.g. different training certifications or professional regulators. We can, of course, support you in locating notices if you require.

International Transfers

To Guernsey

First Central has offices and services that are located outside the UK & EEA and therefore we may need to transfer personal data to other group companies in those countries to perform our activities. These transfers of personal data are considered restricted transfers under the law; therefore, we are obligated to ensure that appropriate transfer and safeguard mechanisms are in place for them to be lawful.

The most common transfer of personal data we will make is providing UK employee personal data to First Central in Guernsey. We are not required to obtain your consent for the transfer of this data, as Guernsey has been granted "adequacy" by the European Union. This means that it has been deemed as having an appropriate and adequate legal framework in place to protect your personal data and your rights and freedoms.

We will, of course, put in place safeguards for these transfers, such as limiting what is being sent to what is necessary and ensuring a standard level of encryption for the transfer and when the personal data is at rest.

To the USA

We utilise technology and software from third parties, some of which are based in the USA. Where possible we will ensure that any transfers of personal data to these third parties remain within EU arrangements, but if that is not possible, the third party must be certified under the EU-USA Privacy Shield framework for the transfer to take place.

We will make sure that any third parties are subject to a contract with us and that an adequate level of technical and organisational security is in place prior to transferring any personal data. In all cases this information is limited to your working data e.g. your name, your work email or job role and access requirements.

Transfer to other countries

If we need to perform an international transfer to any other countries, we will let you know and provide details about the steps we have taken to ensure the privacy and security of your personal data. We will also ensure that such transfers are compliant with the law, by having the legal mechanisms in place for the transfer and appropriate safeguards.

If you have any concerns about your personal data being transferred to another country, contact the Group Data Protection Officer at DPO@first-central.com.

Your rights

The law provides you a number of rights. They are not all “automatic”, meaning they will only apply in certain circumstances. It is important you know your rights and understand when they apply.

The right to be informed

You have the right to be told how First Central will process your personal and sensitive personal data, for what purpose and for how long. This information is provided in this notice, but it is a continuing right; therefore, we will always try to keep things up to date.

This notice will be available to employees on Centranet, in your Select HR account within the GDPR Preference Centre and on our careers website. This document will be reviewed at least annually to ensure that any new activities are captured, and we are being transparent with you. We will also provide access to details of privacy notices from third parties to whom we may have passed your personal data. We want you to be informed and to know who to contact to find out more.

We also provide information in more layered ways, such as using our business communications and training that is provided annually. We may release FAQs about new activities to support your understanding. Information can also be sought directly from the Group Data Protection Officer.

The right to access

You have a right to access the personal data First Central holds about you. This can be requested anytime and there is no fee chargeable. We have 30 days to respond to a request. As part of your request, let us know what information you require.

If you are a current employee, you have access to the data First Central holds within SelectHR, which can be accessed at any time. In fact, we encourage you to check this information regularly to ensure it is accurate.

If you were an employee and left prior to May 2018, your records are now in a physical storage archive. These can be accessed by request to the Group Data Protection Officer, who will facilitate a copy to be made available.

The Group Data Protection Officer may need to redact or exclude certain documentation. If this is the case, you will be told the nature of the document and the reasons why it is being excluded, i.e. the Group DPO will exclude any email communications from you that are sent about our customers.

The right to rectification

You have a right to ask us to update any personal data we hold about you that is inaccurate. As an employee, we will ask you annually to check your details on SelectHR and you can update this information yourself. If you would like other records updated, you should contact HR, who will take the necessary steps to update the information.

The right to erasure

It is important to note that this is not an automatic right and only applies in certain circumstances. This request can be made free of charge and we have 30 days to respond. This time frame can also be extended.

We do need to retain personal data; therefore, we will not comply with a request unless one of the following exceptions applies:

The personal data is no longer necessary for the purpose which we originally collected or used it

When you leave we cease processing of the personal data. We retain your employment records for seven years for, so we can meet out legal obligations and excise or defend any legal claims. After this, all electronic and paper records will be deleted or anonymised.

We are relying on consent as the lawful basis for holding the data, and the employee withdraws their consent

We do not rely on employee consent. If we do for a specific activity, a record of that consent will be stored. If you withdraw your consent for the activity we will stop the activity and can erase the data.

We are relying on legitimate interests as the basis for processing, the employee objects to the processing of their data, and there is no overriding legitimate interest to continue this processing

We rely on legitimate interest to conduct some of our activities. We do this as often the activity is for the employee's benefit. We consider this processing necessary to give our employees the best experience whilst they are here. However, if you do object, let us know and we will consider if there is an overriding interest meaning we can continue or must stop and erase the data.

We are processing the personal data for direct marketing purposes and the employee objects to that processing

We do not currently conduct any direct marketing with our employees, therefore, this reason would not be accepted. If we did, you would have the right to ask us to stop and be removed from the activity.

We have processed the personal data unlawfully (i.e. in breach of the lawfulness requirement of the first principle)

If there is a proven unlawful processing of your personal data, we are obligated to erase your information.

We must do it to comply with a legal obligation

If we receive a court order or we are required under the law to erase the personal data, then we will.

The right to restriction

This right is not often used but is available to you. It means you can limit the way we can use your personal data, but it only applies in the following circumstances:

- You are contesting the accuracy of the personal data and can stop us doing anything whilst that data is verified
- The data has been unlawfully processed (i.e. in breach of the lawfulness requirement of the first principle of the GDPR) and you oppose us erasing it and request restriction instead
- We no longer need the personal data, but you do for legal claims, so we will restrict the use and keep it
- You object to First Central using the personal data for a legitimate interest activity and First Central needs to consider whether the legitimate grounds override your right

If the right is granted, we will stop processing the personal data and place a hold on it. We have one month to respond to a request for restriction.

The right to data portability

You have the right to request data portability where the activity has been done in performance of a contract and was carried out by automated means. We do not currently undertake any automated activities using employee data, however, you can access and obtain a copy of your personal data through SelectHR if you need a copy.

The right to object

You can excise a right to object to an activity in limited circumstances. Again, this is not an absolute right and only applies where direct marketing is undertaken, or the activity is done on a legitimate interest ground. In the latter scenario, you must give specific reasons why you are objecting to the activity. First Central can continue the activity if it can demonstrate a compelling, legitimate ground for it, or if it is necessary for the excise or defence of legal claims.

Rights relating to automated decisions and profiling

You have the right to not be subject to a decision based solely on automated processing (including profiling), which produces a legal or similarly significant effect on you. This can most commonly be seen in e-recruiting practices. We do not currently make automated decisions in this way.

Making the requests

If you would like to make any of the above requests to First Central, you can do so by contacting the Group Data Protection Officer at DPO@first-central.com or to the HR team at Human.Resources@first-central.com.

Retention

We have legal obligations to retain certain personal data we collect about you. Our general approach is to retain the personal data for a period of seven years from the termination of your employment contract.

When you have left the company, your records are moved into archive and only used where strictly necessary, but to ensure we can meet our obligations, they do have to be retained.

Here are some of the requirements we have to follow:

Stage or type of information	**Retention period**
Unsuccessful recruitment – interview and application packs	12 months – suitability for other roles
End of employment – your personnel file	7 years - litigation time limits
Health and safety – accidents logs	3 years - RIDDOR 1995
Redundancy 20 or more employees – facts relating to	12 years – Limitation Act 1980
Salary records – payroll	7 years – Taxes Management Act 1970
Medical records (under COSHHR)	40 years – COSHHR 2012

Right to complain

We hope you never have to, but if you are unhappy with how we have used your personal data or are concerned about the security or sharing of your information, you should raise your concerns to the HR team or the Group Data Protection Officer in the first instance.

Every concern raised is investigated and a final response will be provided.

You also have the right to lodge your complaint with the Supervisory Authority in your country of employment. This could be the Information Commissioner in the UK, the Guernsey Office of Data Protection or the Gibraltar Regulatory Authority.

They will contact us and ask us to review how we have handled your concerns.

Definitions

The following words in this notice have the following meaning:

Word	Definition
First Central Group of Companies	First Central Insurance Management, Skyfire Insurance Company, First Central Group, First Central Services UK, First Central Services Guernsey and Skyfire Reinsurance Company.
Personal data	Any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Special Personal data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation and criminal convictions.
Activity	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Controller	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
Processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Legal Ground	The lawful grounds defined in Article 6 of GDPR and other applicable sections of legislation.

Consent	Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
Supervisory Authority	An independent public authority which is established by a Member State, such as the Information Commissioner's Office, Gibraltar Regulatory Authority or the Guernsey Office of Data Protection.
Retention	The length of time we will hold onto a copy of your personal data.
Third Parties	A natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.
Profiling	Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular, to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.