Privacy policy

Classification: Public
Region: International
Type: Policy
Document Owner: Risk & Regulation
Last Review Date: 11 April 2024
Next Review Date: 13 February 2025
Version Control: 9.0a Final

sedgwick®

Table of contents

Version control

Version	Date	Comment
V7.5	25/10/2022	Superseded
V8.0	13/10/2023	Annual review and general update
V9.0a	11/04/2024	Update to include reference to EU-US DPF and UK bridge, including hyperlink to the Sedgwick Data Privacy Framework notice. Correction to email address.

Scope

This policy document relates to all Sedgwick International colleagues, including its subsidiaries and affiliates.

Applicability

This policy applies to all Sedgwick colleagues; including temporary staff, contractors, sub-contractors and authorised third parties.

Introduction

In delivering most of our services Sedgwick and its subsidiaries acts on behalf of an insurer and/or insurance broker. In that situation the privacy policy of the insurer and/or insurance broker will apply as they will be the controller of the data we process on their behalf. If you are uncertain, we will always be here to help you identify the party that controls your data.

Sedgwick is committed to protecting the privacy of Personal Data we collect and process in conducting our business. “Personal Data” is information that identifies you, or other individuals (such as your dependents).

This Privacy Policy describes how we handle Personal Data that we collect through:

- Delivery of our “Services”
- Claim or other forms, surveys, telephone calls, e-mails, webchat and other communications with us, as well as from (claim) investigators, medical professionals, witnesses or other third parties involved in our dealings with you
- Our websites (the “Site”)
- Our software applications (the “Apps”)
- Our (pre-)employment arrangements

Collectively referred to as the “Processes”.

We collect and process your Personal Data in accordance with this Privacy Policy, which also includes details about our use of website cookies in line with current data protection legislation including the General Data Protection Regulation 2016/679 (GDPR).

For information on your rights and how Personal Data is collected, stored and processed as part of Services go to the 'Our operational services' section of this policy.

Who to contact about your Personal Data

If you have any questions about our use of your Personal Data you can contact our Data Protection Officer:

Anne Brett

Merrion Hall
Strand Road
Sandymount
Dublin 4
Ireland

Email: DPOinternational@ie.sedgwick.com

Email contacts below:

Region	Email Address
UK	dataprotection@uk.sedgwick.com
Ireland	Dataprotection@ie.sedgwick.com
Netherlands	privacy@nl.sedgwick.com
Germany	privacy@nl.sedgwick.com
Spain	privacy@nl.sedgwick.com
Belgium	privacy@nl.sedgwick.com
Denmark, Sweden and Norway	privacy@nl.sedgwick.com
France	protectiondesdonnees@fr.sedgwick.com

The postal address for our Head office is:

Data Protection Officer

Sedgwick Corporate
3030 North Rocky Point Drive West
Suite 530
Tampa, Florida 33607

Our EU Representative, appointed pursuant to Article 27 GDPR, is Sedgwick Outsource Services Ireland Limited. It may be contacted at:

Sedgwick Outsource Services Ireland Limited
Merrion Hall
Strand Road
Sandymount
Dublin 4
Ireland

The UK Representative of Sedgwick Claims Management Services, Inc., is Sedgwick International UK. It may be contacted at:

Sedgwick International UK
30 Fenchurch Street
London
EC3M 3BD

Personal Data we collect and process

The Personal Data we gather about you, your dependents and others will depend on the type and nature of the service we are providing, but may include:

General identification and contact information

- Your name, address, e-mail and telephone details, gender, marital status, family status, date and place of birth, educational background, physical attributes, activity records, driving records, photos and video images, employment history, skills and experience, professional licenses and affiliations, occupation, employer, lifestyle, internet profile, social media, credit status, electoral data, County Court Judgements (CCJs), security measures, relationship to the policyholder, insured or claimant, and date and cause of death, injury or disability.
- Identification numbers issued by government bodies or agencies - Social Security or national insurance number, passport number, tax identification number, military identification number, driver's or other license numbers

Financial information and account details

- Bank account number and account details, credit history and credit score

Medical condition and health status

- In certain situations, we may process information about your current, or former, physical, mental or medical conditions, health status, injuries or disabilities, medical procedures performed, personal habits (for example, smoking or consumption of alcohol), prescription information and medical history

Other sensitive or special category information

In certain situations we may also process sensitive information about your trade union membership, religious beliefs, political opinions, family medical history or genetic information (for example, if you applied for insurance through a third-party marketing partner that is a trade, religious or political organisation)

- We may also obtain information about your criminal record or civil litigation history
- We may also obtain sensitive information if you voluntarily provide it to us (for example, if you express preferences regarding medical treatment based on your religious beliefs)
- Telephone recordings
- Recordings of telephone calls to our staff and offices

- Telephony information used to investigate crime, including fraud and money laundering: For example, insurers commonly share information about their previous dealings with policyholders and claimants for this purpose

Information enabling us to provide our services

- Location and identification of insured property (for example, property address, vehicle license plate or identification number)
- Travel arrangements, including reservation numbers, destination and hotel details
- Policy details and claim numbers, details of policy coverage and cause of loss
- Data relating to the circumstances, cause and value of an insurance claim and any information that may be relevant to insurer's acceptance of the claim or continuing cover if you are insured with them.
- Prior accident or loss history,
- Your status as director or partner, or other ownership or management interest in an organisation
- Other insurance policies you hold.

Marketing preferences and customer feedback

- You may let us know how you want to be contacted (e.g. by email, phone or post)

How we use your Personal Data

We use the Personal Data we process to:

- Communicate with you and other parties involved in the delivery of our Services
- Send and receive administrative information regarding your casefile, or any other service we are providing to you
- Make decisions about your casefile, for instance regarding (claim) assessment, processing and settlement
- Use with data analytics, modeling (such as predictive modeling), and the deployment of automated tools not creating a significant legal impact to you, and to use the results of such analysis, models, and tools for the purposes otherwise outlined in this Policy.
- Manage and resolve disputes
- Provide improved quality, training and security (e.g. use of recorded or monitored phone calls)
- Prevent, detect and investigate crime, including fraud and money laundering, and analyse and manage other commercial risks
- To determine the extent of liability under an insurance claim and, where appropriate, arrange repairs, replacement or payment. The processing is generally needed to validate:
    - Details of those involved with the claim
    - Details that have been given to us, insurers or other parties
    - The circumstances, cause and value of the claim
    - Any matters that may be relevant to insurers acceptance of the claim

The way we process that data will generally be governed by the contract under which we are appointed

- Carry out scientific, historical, statistical or other market research and analysis, including satisfaction surveys.
- Manage our business operations to comply with internal policies and procedures, including those relating to auditing finance, accounting and billing, IT systems, information security, data and website hosting, business continuity, document and print management
- Resolve complaints, and handle data subject right requests
- Comply with applicable laws and regulatory obligations (including laws outside your country of residence), such as those relating to anti-money laundering and comply with legal process and respond to requests from public and government authorities (including those outside your country of residence)
- Establish and defend legal rights, protect our business operations (including our group companies), our rights, privacy, safety of colleagues and property, you or others related to the claim and pursue available remedies to limit our damages.

We will only process personal data for the purposes set out above, or for any other purposes specifically permitted by applicable data protection legislation. When we act as the controller of your personal data, we will notify you of those purposes when we start processing your personal data, or as soon as possible thereafter.

The personal data processed when you interact with our Services will, in the normal course of our activities, be shared with the parties involved in providing the Services (e.g. our client, and Sedgwick group companies) for the purposes set out in this Privacy Policy and will not be transferred to other individuals or businesses for their own use, unless required by law.

We may also share your personal data with specific vendors, or other entities with whom we have a business relationship, to provide products or services.

We may, as a matter of law, and without requiring notice or consent, use your information for crime and fraud prevention, or systems administration within the Sedgwick group and to monitor and/or enforce Sedgwick's compliance with any regulatory rules and codes.

Notifying Data Subjects

If we collect your personal data directly from you as a data controller, we will inform you about:

The purpose, or purposes, for which we will be processing your personal data

- The types of third parties, if any, with which we may share, or to which we will disclose, your personal data.
- The means, if any, by which you can limit our use and disclosure of your personal data.

If we receive personal data about you from other sources, and this source has not informed you in advance, we will provide you with this information as soon as possible thereafter.

Where we are the data controller we will advise you of the name and contact details for our Data Protection Officer, and how you can exercise your rights as a data subject, including the right to object to the processing of your personal data when it is processed based on legitimate interests.

International transfer of Personal Data

Due to the global nature of our business we may need to transfer Personal Data to parties located in other countries (including, but not limited to, the United States and India) that have a different data protection regime than the country where you are based. For example, we may transfer Personal Data in order to process international travel insurance claims and provide emergency medical assistance services when you are abroad, or we may transfer information internationally to our group companies, service providers, business partners and governmental or public authorities in order to perform our services and/or for the purpose of administering employment terms and benefits.

If we transfer any of the personal data we hold to a country outside the European Economic Area ("EEA") we will ensure that one or more of the following conditions applies:

The country to which the personal data is transferred ensures an adequate level of protection for the data subjects' rights and freedoms

- The data subject has given their consent
- The transfer is necessary for one of the reasons set out in the regulation, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject
- The transfer is legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims
- The transfer is lawfully undertaken through the use of an appropriate transfer mechanism such as standard data protection clauses adopted by the European Commission, on condition that enforceable data subject rights and effective legal remedies for data subjects are available
- The transfer is authorised by the relevant data protection authority, where we have adduced adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights

Subject to the requirements in this clause, personal data we hold may also be processed by staff operating outside the EEA who work for us, or for one of our suppliers. Those staff may be engaged in, among other things, the fulfilment of contracts with the data subject, the processing of payment details and the provision of support services.

EU-US Data Privacy Framework and UK Bridge

Sedgwick Claims Management Service Inc., CareWorks Managed Care Services Inc., York Risk Services Group and EFI Global Inc. adheres to the principles of the EU-U.S. Data Privacy Framework (EU-U.S. DPF) and the UK extension to the EU-U.S. DPF, as set forth by the U.S. Department of Commerce. The Sedgwick entities listed above may rely on the EU-U.S. DPF as a lawful basis for transfers of personal information. To learn more, visit our 'Data Privacy Framework Notice'.

Sedgwick will also continue to rely on the SCCs for the purposes of transfers of personal data from the EU and UK to the US, where applicable. For further information please see International Data Transfers section above.

Sharing of Personal Data

We may make Personal Data available to the following parties for the purposes of providing our Services, or as required by law:

- Our group companies
- Our instructing client:
  - This will often be an insurance company
- Other insurance and distribution parties:
  - While processing your casefile, we may make Personal Data available to third parties such as reinsurance brokers, appointed representatives, distributors, financial institutions, securities firms and other business partners
- Our service providers
  - External third-party service providers, such as medical professionals, accountants, actuaries, auditors, experts, lawyers and other outside professional advisors; travel and medical assistance providers
  - IT systems, support, information security and hosting service providers, document and records management providers and outsourced service providers that assist us in carrying out business activities.
  - Banks and financial institutions that service our accounts, third-party claim administrators, claim investigators, construction consultants, engineers, examiners, jury consultants, translators and similar third-party vendors
- Authorities and third parties involved in court action
  - We may share Personal Data with government or other public authorities (including, but not limited to, workers' compensation boards, courts, law enforcement, tax authorities and criminal investigations agencies); and third-party civil legal process participants and their accountants, auditors, lawyers and other advisors and representatives as we believe to be necessary or appropriate:
    - to comply with applicable law and regulations, including those outside your country of residence
    - to comply with legal process
    - to respond to requests from public and government authorities including public and government authorities outside your country of residence
    - to protect our operations, or those of any of our group companies
    - to protect our rights, privacy, safety or property, and/or that of our group companies, you or others
    - to allow us to pursue available remedies or limit our damages.
- Other Third Parties
  - We may share Personal Data with emergency providers (fire, police and medical emergency services); retailers; medical organisations and providers; Employment tribunal; Benefits entities; travel carriers; credit bureaus; credit reporting agencies; and other people involved in an incident that is the subject of a claim; as well as purchasers and prospective purchasers or other parties in any actual or proposed reorganisation, merger, sale, joint venture, assignment, transfer or other transaction relating to all or any portion of our

business. To check information provided, and to detect and prevent fraudulent claims, Personal Data (including details of injuries) may be put on registers of claims and shared with other insurers. We may search these registers when dealing with claims to detect, prevent and investigate fraud.

- For Sedgwick colleagues personal data, where we act as a Data Controller, we may share your personal data with other companies in the Sedgwick group, our contractors, vendors/supplier, agents, or other known third parties (such as banks, insurers, brokers, clients, auditors, benefit providers, pension providers, background screening providers and educational bodies and institutes) to carry out our obligations under employment law, our employment contract with you, in the provision of our service or for our legitimate interests.

Security of Personal Data

We will take all appropriate reasonable technical, legal and organisational measures, which are consistent with applicable privacy and data security laws, to safeguard your Personal Data. Unfortunately, no data transmission over the Internet, or data storage system, can be guaranteed to be 100% secure. If you have reason to believe that your interaction with us is no longer secure (for example, if you feel that the security of any of your Personal Data held by us has been compromised), please notify us immediately.

Where we provide any of your Personal Data to a vendor, the vendor will be selected carefully and required to use appropriate measures to protect the confidentiality and security of that Personal Data.

Accuracy of Data

We take all reasonable steps to ensure that Personal Data we process remains accurate and complete as is necessary for the performance of our services to you and in line with the controls detailed in this Privacy Policy.

Retention of Personal Data

We will retain Personal Data for the period necessary to fulfil the purposes outlined in this Privacy Policy unless a longer retention period is required or permitted by law.

Personal Data of other Individuals

If you provide Personal Data to us regarding other individuals, you agree:

- to inform the individual about the content of this Privacy Policy
- to obtain any legally required consent for the collection, use, disclosure, and transfer (including cross-border transfer) of Personal Data about the individual in accordance with this Privacy Policy

We request that children do not provide us with any personal information through the Site or the Apps.

Access and Correction Requests, Questions or Concerns

In certain countries, an individual may have the right to access, correct or object to the use of, or request deletion or suppression of Personal Data on certain grounds. Please contact us as set out in the "Who to Contact About Your Personal Data" section above with any such requests, or if you have any questions or concerns about how we process Personal Data. Please note that some Personal Data may be exempt from access, correction, objection, deletion or suppression rights in accordance with local privacy and data protection laws.

Other Information We Collect

"Other Information" is information that does not reveal your specific identity, such as:

- App usage data
- Information collected through cookies, tags and other technologies

We and our third-party service providers may collect "Other Information" in a variety of ways, including:

- Through your use of the App: When you download and use the App, we and our service providers may collect App usage data, such as the date and time the App on your electronic device accesses our servers and what information and files have been downloaded to the App based on your device number

Using cookies: Cookies are pieces of information stored directly on the computer you are using. For a full list and more information with respect to cookies we use please refer to the privacy policy linked on our main Sedgwick.com page.

These cookies are used to collect information about how visitors use our site. We use the information to compile reports and to help us improve the site. The cookies predominantly collect information in an *anonymous form*, including the number of visitors to the site, where visitors have come to the site from and the pages they visited.

Third Party Services

This Privacy Policy does not address, and we are not responsible for, the privacy, information, or other practices, of any vendors, including any vendor operating any site or service to which the Services link. The inclusion of a link on the Services does not imply endorsement of the linked site or service by us, or by our group companies. Before providing any Personal Data to any such linked website, please make sure you review that website's privacy policy carefully to understand how it deals with your Personal Data.

Consent to use Personal Data

We will inform you when we require your consent to process your personal data and will request it from you as outlined in this Privacy Policy. If you do not provide that consent when requested, we may not be able to provide you with our Services. If necessary, please contact us as set out in the "Who to Contact About Your Personal Data" section above for further information.

Our operational services

This section relates solely to the provision of our Services

What we do

Our use of your personal data depends on the type of service we are providing and your relationship with our organisation. It may also be governed by the contract we have with the party for whom we are acting.

Sedgwick primarily provides Services related to insurance policies arranged with the insurance sector, or organisations operating in a similar capacity, hereinafter referred to as the insurer.

Our Services include:

- Loss adjusting and claims handling
- Client support services including sales, training and educational activities
- Call centre services
- Customer services
- Debt recovery and collection
- Recourse claims
- Policy administration
- Surveys of buildings or other (potential) incident related items
- Fulfilment services, to return an individual to their position prior to the incident
- Valuations
- Specialist analysis, such as medical or financial
- Forensic and fraud investigations
- Recruitment and secondment
- Other related services

When performing loss adjusting or claims handling for insurers, our primary function is to establish the extent of their liability for a claim. Once we have completed our enquiries we either report back to the insurer with our findings, or make recommendations for payment, repair or replacement as appropriate.

Under some arrangements, we may be able to conclude matters without referring to insurers, known as “Delegated Authority.”

In order to perform all these activities, we need to process personal data.

Personal data

Personal data means information relating to an identified or identifiable natural person (data subject). 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.

Processing

Processing personal data means 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, organisating, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data Controller / Processor

A data controller means a natural or legal person which, alone or jointly with others, determines the purposes, and means of the processing of personal data.

A data processor means a natural or legal person which processes personal data on behalf of the controller.

Unless otherwise advised, Sedgwick will be a processor of your data. However, this may vary depending on our relationship with you and the contractual arrangements of the client we are working for.

As an employer, Sedgwick usually operate as the Data Controller for our colleague's personal data.

Please also note we sometimes act in the name of our client, regardless of whether we are a processor or controller.

Legal Basis for Processing

For personal data to be processed lawfully, it must be processed by the Data Controller based on one of the lawful bases set out in the relevant regulation/legislation. These include:

- The legitimate interest of the data controller or the party to whom the data is disclosed, or;
- The processing is necessary for the performance of a contract, or;
- Processing is necessary in order to protect the vital interest of the data subject, or;
- Processing is necessary for the performance of a task carried out in the public interest, or;
- The compliance with a legal obligation to which the data controller is subject, or;
- The data subject's consent to the processing.

When special category (sensitive) personal data is being processed additional conditions must also be met.

When processing personal data as data controllers, we will ensure that all regulatory and legislative requirements are met. Depending on your relationship with our organisation the legal basis for us processing special category data will be one of the following:

- Processing is necessary for the performance of a contract, or legal duty
- Processing is necessary for a legitimate interest pursued by our client, us, or a third party
- Processing is necessary for the purposes in the field of employment
- Processing is necessary for the establishment, exercise or defence of legal claims

- Processing is necessary for the assessment of the working capacity of the data subject, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services
- Processing is necessary for settling claims for benefits and services in the insurance system
- Processing is necessary for substantial public interest,
- Processing is necessary to protect the vital interests of the data subject
- Processing relates to personal data which are manifestly made public by the data subject
- Processing is necessary for archiving purposes, scientific or historical research purposes or statistical purposes
- You have given (explicit) consent to us, or the party for whom we are acting

Where we use legitimate interest as our grounds for processing your data you have the right to object to that processing at any time.

Purpose of Processing

The purpose for which we will use personal data will depend on your relationship with our organisation. For our primary service, of claim handling, the intended purpose is to determine the extent of liability for a claim and where appropriate, arrange repairs, replacement or payment.

We will only use the personal data we collect for the purpose of delivering our Services and for no other purpose.

Consent

In most cases we do not need to obtain consent to process your personal data as this will not be the legal basis we will rely for such processing. We will inform you if we require your consent to process your personal data and will request that you provide us with your consent as outlined in this Privacy Policy.

If you do not consent, we may not be able to provide you with our services. If necessary, please contact us as set out in the “Who to Contact About Your Personal Data” section above for further information.

Requirement for you to Provide Data

Generally, a contract of insurance will require your co-operation in providing information about your casefile, including any personal data. The precise wording will depend on your policy or contract.

If you are a third-party claimant, there is no requirement on you to provide us with your personal data. However, failure to do so is likely to prejudice your right to claim either under a policy, or under contract, or in law.

In relation to our other services it is likely that if you do not provide us with your personal data we will not be able to provide you with our services.

Background Checks

The nature of our work is such that we may need to make background enquiries regarding colleagues or individuals connected with a casefile to validate information we are given, satisfy contractual obligations, comply with regulatory or legal requirement, or to combat fraud, financial crime and money laundering. As part of the validation process we may check with other organisations, including credit reference agencies, data providers and other parties who may assist in validating the casefile or providing our Services.

Sources of Personal Data

At the outset of providing our services we usually receive basic information about you direct from our instructing client. Depending on the type and nature of the service we are being asked to provide we might then have to gather additional information from other sources such as:

Credit reference agencies, claim industry databases, local and public authorities, services and agencies, health service, healthcare providers, government, the internet, social media, crime prevention agencies, police, fire brigade, suppliers, valuers, vendors, witnesses, friends, relatives, acquaintances and any other person or organisation that might assist with providing our service.

Automated Profiling & Decision Making

As part of the services we provide, we may need to analyse, or process, your personal data automatically to indicate the best way of handling the casefile. However, any such profiling or decision making that has legal effects concerning you, or similarly affects you, will not be relied on exclusively without human intervention or taking other factors into consideration.

Your Right to Rectification

You have the right at any time to request that we correct any inaccurate personal data we hold about you. We want our records to be as accurate as possible, so please advise us of any errors. However, please note that a difference of opinion or view is not necessarily inaccurate data and changes might not be possible. However, should you wish to express your own views, please provide details or a statement and we will add them to our records. Where this is required, please communicate the corrections or supplements to those dealing with your casefile.

If necessary, please contact us as set out in the “Who to Contact About Your Personal Data” section above for further information.

Erasure and your “Right to be Forgotten”

You have the right to have your data deleted when it is no longer needed, which is known as the “Right to be forgotten.” However, we have an obligation to keep records for audit, regulatory and legal purposes and to combat financial crime.

To meet these obligations, we keep records in accordance with our Retention Policy. Consequently, we may not be able to delete records when requested, or when a claim has been finalised. However, in certain circumstances we may be able to “Restrict Processing”. We may be able to delete specific data, or a document, for example where it has been sent to us in error and this will be done without undue delay.

In the first instance, please speak to those handling your casefile to see if they can assist.

If necessary, please contact us as set out in the "Who to Contact About Your Personal Data" section above for further information.

Your Right to Withdraw Consent

You have a right to withdraw consent to processing your personal data in certain circumstances. This will only apply where we are relying on your consent to process your personal data. If we are relying on your consent, then withdrawing it is likely to prevent us providing our Services and, if related to claims handling, we may be unable to settle your claim. Should you wish to exercise your right, please put this in writing (email is also acceptable) to those handling your casefile.

Please also note that if you object or withdraw consent, we might still need to process your data to resolve ongoing commitments and satisfy obligations detailed under "Erasure and your Right to be Forgotten."

If necessary, please contact us as set out in the "Who to Contact About Your Personal Data" section above for further information.

Your Right to Object to Processing

The law gives an individual the right to object to the processing of their personal data:

- For purposes of direct marketing - we do not ordinarily do this so it will not generally apply
- Solely based on legitimate interests pursued by us, or a third party, or a task in the public interest - please note that this right does not apply if we are processing your data for the performance of a contract e.g. a claim under an insurance policy
- For scientific or historical research and statistics - we do not ordinarily do this so it will not generally apply

Any objection on the above grounds should be communicated to our operational team managing the service we are providing so they can refer your request to our data protection department.

If necessary, please contact us as set out in the "Who to Contact About Your Personal Data" section above for further information.

Right to Restrict Processing

When requested we will restrict processing where:

- You contest the accuracy of the personal data that we are processing. However, please note that:
    - a difference of opinion or view does not necessarily constitute inaccurate data
    - the restriction will only apply to the personal data in dispute rather than all the information we hold in the casefile. When a restriction is put in place, we will not process the data in question other than to resolve its accuracy during which time the restriction will be noted on our system

- Processing is unlawful and to prevent erasure you demand a restriction of processing instead. If the processing is unlawful, we will place a restriction on the record and, if requested, preserve the data
- We are due to delete your personal data, but you request that we preserve it for the establishment, exercise or defence of a legal claim
- You object to us processing your data where our only grounds for doing so are either a task in the public interest, or a legitimate interest pursued by us or a third party. We will then restrict processing pending verification of whether we have overriding grounds for processing

In each case we will inform you before any restriction is lifted. However, please note:

- Even with a restriction in place we are still allowed to store data and process it for the establishment, exercise or defence of legal claims, or for the protection of the rights of another natural or legal person
- A restriction only applies to personal data or part of it and we can continue processing other data regarding your casefile
- We will not be responsible for any delay in provision of our services caused by unnecessary restrictions imposed by you

Your Right to Access Data

Under the GDPR, you have a right to request a copy of your personal data that we hold by making what is known as a "Subject Access Request" or SAR. In many instances the information you are seeking will be available without the need for making a formal SAR. You should therefore start by asking those liaising with you over our service provision for the information you are seeking as this will avoid the possible delay of a formal SAR. The GDPR allows us a month to respond which can be extended by a further two months, where necessary, taking into account the complexity and number of requests.

If you do make a formal SAR, where we act as the data controller, we will review the information we hold to ascertain what personal data can be provided. If we are acting as a data processor, we will forward the SAR to the data controller, normally our instructing client.

Please note that when responding to a SAR certain data might be subject to exceptions and exemptions, depending on the situation and nature of your casefile.

Should you wish to pursue a formal SAR, please inform the Sedgwick team liaising with you over our service provision as this will speed up your identification. Alternatively, the request can be directed to the relevant Data Protection Department at Sedgwick, as set out in the "Who to Contact About Your Personal Data" section above.

If you submit a SAR, we will advise you of the next steps as soon as possible.

Telephone call recording

Please be aware that our organisation may record telephone calls for training, security purposes, fraud detection and prevention. However, we do not record telephone calls at all our offices and there may be no recording where our staff work remotely or use mobile phones.

Call recordings are retained for a limited period, depending on the service being provided, any contractual requirements with those we are working for and the technical facilities in place.

Right to data portability

You have the right to receive the personal data, that you have provided to us in a machine-readable format or when requested, we can also send it to another data controller where this is technically feasible. However, please note:

- portability only applies to the data you have provided to us rather than your complete casefile
- portability only applies to data capable of being converted into machine-readable format, which may exclude images, scanned document, photographs etc. that you have provided
- portability is only available where:
  - processing is based on consent, or for the performance of a contract, and;
  - the processing is carried out by automatic means

However, should you want to exercise your right under this option, please advise those liaising with you over our service provision.

Transferring data outside European Union

We are a global business and may need to transfer, store or process your data on systems, or in parts of our organisation, outside the European Union. However, we will ensure that any such activity is subject to a lawful transfer mechanism and appropriate levels of information security and data protection measures necessary to comply with the law applicable within the European Union.

For further information please refer to 'International transfer of Personal Data' section of this Privacy Policy.

Right to complain

Should you consider that our organisation has not complied with relevant data protection law, you have a right to take legal action or to complain to our Lead Supervisory Authority.

Our organisation's Lead Supervisory Authority is the Data Protection Commission, based in Ireland, details below:

Their website is: https://www.dataprotection.ie/

Or, you can call their helpline

- between 10:00 - 12:00hrs (Monday - Friday) on 076 110 4800
- between 14:00 - 16:00hrs (Monday - Friday) on 057 868 4800

Or, you can write to them at:

Data Protection Commission

21 Fitzwilliam Square South

Dublin 2

D02 RD28

Ireland

Time frame for responding to requests

We will seek to respond to any request we receive in relation to your rights within one month. However, if this is not possible, we will advise you within one month that the time frame will be extended by up to a further two months and give an explanation why the extension is required.

Charges/fees

Our response to and any actions necessary for us to comply with a request by you in respect of any of your rights will be handled free of charge to you. The only exception to this will be if the request is excessive or repetitive. If we do intend making a charge, we will inform you of this before proceeding with any actions that might incur that charge.

Recruitment

Introduction

Sedgwick (the "Company") holds personal data on job applicants. That means the Company is a data controller and determines the purpose and means of the processing of your personal data.

This Privacy Notice describes:

- how the Company holds and process your information, including special categories of personal data, in accordance with our obligations under the GDPR
- how the Company seeks to protect the personal data of job applicants who are situated in Europe during the recruitment process; and
- your rights as a data subject.

The Company takes the security and privacy of your data seriously. We need to gather and use information or 'data' about you as part of the recruitment process. We comply with our legal obligations under the GDPR and the laws in the country in which you applied for a position with us in respect of data privacy and security.

This Privacy Notice applies to all personal data whether it is stored electronically, on paper or on other materials.

Data Processing Activities

We will only hold data for as long as necessary for the purposes of the recruitment process.

Your personal data will be kept for six months after the conclusion of the recruitment process unless you agree to a longer retention period.

The personal data might be provided to us by you, or someone else (such as a former employer or recruitment agency), or it could be created by us.

We may collect and use the following types of personal data about you: your application form, CV, references, qualifications and membership of any professional bodies and details of any pre-employment assessments.

We will use your personal data for:

- complying with any legal obligation;
- the normal course of pre-employment contracting during the recruitment process
- our legitimate interests while conducting the recruitment process. However, we can only do this if your interests and rights do not override ours. You have the right to challenge our legitimate interests and request that we stop this processing.

We can process your personal data for these purposes without your knowledge or consent.

We will not use your personal data for an unrelated purpose without telling you about it and the legal basis that we intend to rely on for processing it.

We will process your personal data in various situations during your recruitment process, for example:

- to decide whether to employ (or engage) you
- to decide how much to pay you, and the other terms of your contract with us
- to check you have the legal right to work for us
- to determine whether we need to make reasonable adjustments to your workplace or role because of your disability
- to monitor diversity and equal opportunities;
- to comply with employment law, immigration law, health and safety law, tax law and other laws which affect us
- the prevention and detection of fraud or other criminal offences
- for any other reason which we may notify you of from time to time

In some cases, we may need your consent for processing your personal data. This will usually involve processing special categories of your personal data (for instance, health and criminal data). If we ask for your consent to process your personal data, then we will explain the reasons for our request. You do not need to consent and can withdraw your consent later if you choose by contacting our Data Protection Office.

If you choose not to provide us with certain personal data, you should be aware that we may not be able to carry out certain parts of our recruitment process in a normal fashion or, we might create dangerous or unsuitable situations, where relevant information has not been provided to us. For instance, informing us about an illness or medication might save your life at some point, or informing us about being in a wheelchair will allow us to make reasonable adjustments for carrying out your interview (choose a specific office or floor that does have an elevator or ramp).

We do not need your consent to process special categories of your personal data when we are processing it for the following purposes, which we may do:

- where it is necessary for carrying out rights and obligations under employment law
- where it is necessary to protect your vital interests or those of another person where you/they are physically or legally incapable of giving consent
- where you have made the data public

- where processing is necessary for the establishment, exercise or defence of legal claims
- where processing is necessary for the purposes of occupational medicine or for the assessment of your working capacity.

For some positions we may obtain, or ask you to obtain, a certificate from the relevant criminal background check agency if permissible under local laws. This is usually where the position requires you to deal face to face with members of the public, including visiting their homes, or where the position is one of trust.

Sometimes we might share your personal data with group companies or our contractors and agents to carry out the recruitment process.

We require those companies to keep your personal data confidential and secure and to protect it in accordance with the law. They are only permitted to process your data for the lawful purpose for which it has been shared and in accordance with our instructions.

Your data subject rights

- You have the right to information about what personal data we process, how and on what basis as set out in this Privacy Notice
- You have the right to access your own personal data by way of a subject access request. To do so, you can contact our Data Protection Office
- You can correct any inaccuracies in your personal data. To do so, you can contact our Data Protection Office
- You have the right to request that we erase your personal data where we are not entitled under the law to process it or it is no longer necessary to process it for the purpose it was collected. To do so, you can contact our Data Protection Office
- While you are requesting that your personal data is corrected or erased or are contesting the lawfulness of our processing, you can apply for its use to be restricted while the application is made. To do so, you can contact our Data Protection Office
- You have the right to object to data processing where we are relying on a legitimate interest to do so and you think that your rights and interests outweigh our own and you wish us to stop.
- You have the right to complain to your local Data Protection Authority. This will depend on which Country, or even which administrative region you live or work in.

Changes to this Privacy Policy

We review this Privacy Policy regularly and reserve the right to make changes at any time to take account of changes in our business and legal requirements. We will place updates on our website.