

**Privacy Information Notice**  
**Goldman Finch Limited**

Version: September 2026

The table below provides a summary of the key information in this notice. Full details follow in the sections beneath.

|                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Who we are</b>                    | Goldman Finch Limited (“GFL”), 17 Prospect House, Colliery Close, Staveley, Chesterfield S43 3QE. SRA No. 816551. ICO No. <b>ZB514670</b> .                                                                                                                                                                                                                                                                                                         |
| <b>Data Protection Officer</b>       | Jonathan Whittle — dataprotection@goldmanfinch.com                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>What personal data we collect</b> | Name, address, date of birth, contact details, and (where relevant to your claim) financial, medical, employment and other records. See full notice for details.                                                                                                                                                                                                                                                                                    |
| <b>Why we collect it</b>             | To assess and pursue your legal claim under your retainer with us; to evaluate pre-retainer enquiries; to comply with legal obligations (including UK sanctions law); and for legitimate business purposes including defending claims against us.                                                                                                                                                                                                   |
| <b>Lawful bases</b>                  | Contract (retainer); Legitimate interest (including recruitment); Legal obligation (sanctions screening); Consent (electronic direct marketing, and explicit consent for automated eligibility scoring of certain claims). Legitimate Interest Assessments are carried out where we rely on legitimate interest.                                                                                                                                    |
| <b>How long we keep it</b>           | 15 years from conclusion of your matter or initial enquiry (up to 25 years for limited suppressed contact data thereafter). 6 years for recruitment data. See full notice for details.                                                                                                                                                                                                                                                              |
| <b>Who we share it with</b>          | Courts, opponents, experts, barristers, third-party processors and platforms. See full notice for details.                                                                                                                                                                                                                                                                                                                                          |
| <b>International transfers</b>       | Some personal data is transferred outside the UK via WhatsApp (Meta), Google Drive and Microsoft OneDrive/SharePoint under the UK Extension to the EU–US Data Privacy Framework; and via our AI tools, Claude (Anthropic) and Microsoft Copilot, under the EU Standard Contractual Clauses and UK International Data Transfer Addendum. See "International Transfers of Personal Data" and "Use of Artificial Intelligence" below for full details. |
| <b>Your rights</b>                   | Access, rectification, erasure, restriction, portability, objection, and rights relating to automated decision-making. Contact us or the ICO at <a href="http://www.ico.org.uk">www.ico.org.uk</a> / 0303 123 1113.                                                                                                                                                                                                                                 |

|                                  |                                                                                                                                                                                                                                                                                                                      |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Automated decision-making</b> | With your explicit consent, we use an automated scoring process to assess eligibility for certain group claims; this can result in your claim being closed without individual review. See "Use of Artificial Intelligence" and "Your Data Protection Rights" for full details, including your right to human review. |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

In pursuance of your claim, by making an enquiry about pursuing a claim, by applying for a position with us, or by engaging with us on social media, by telephone or via our websites, personal data about you will be held by Goldman Finch Limited ("GFL") of 17 Prospect House, Colliery Close, Staveley, Chesterfield, S43 3QE, and we shall determine the purpose and means by which that personal data is processed. We are a data controller within the meaning of the Data Protection Act 2018 ('DPA') and the UK General Data Protection Regulation ('UK GDPR').

Jonathan Whittle is GFL's Data Protection Officer. He can be contacted at [dataprotection@goldmanfinch.com](mailto:dataprotection@goldmanfinch.com).

This document explains our role as a data controller and the personal data that will be processed in pursuance of your claim.

The UK GDPR provides the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

It is important to note that the rights available to you under the UK GDPR depend upon the lawful bases for which we process the personal data. As such, not all rights are available to you in all circumstances.

We reserve the right to update this Privacy Information Notice periodically, and you should check this policy on a regular basis to ensure you are aware of the most recent version. Where a change materially affects how we process your personal data — as with the introduction of AI-assisted processing described in this version — we will take reasonable steps to notify existing clients and current enquirers directly, in addition to publishing the updated notice on our website.

### **What is Personal Data?**

The UK GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified, in particular by reference to an identifier such as a name, identification number, location data or online identifier.

The UK GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. Personal data that has been pseudonymised may also fall within scope, depending on how difficult it is to attribute the pseudonym to a particular individual.

The UK GDPR refers to sensitive personal data as "special categories of personal data". These include genetic data (which is always a special category), and biometric data where processed for the purpose of uniquely identifying an individual.

## **Processing of Personal Data at the Enquiry Stage**

If you submit personal data to us before entering into a retainer — for example by completing an online enquiry form, contacting us by telephone, email, live chat or social media, or by any other means — we will process that personal data in order to assess whether we are able to act for you and to consider the merits of any potential claim. Our lawful basis for processing personal data at this stage is legitimate interest: GFL has a legitimate interest in receiving and evaluating information submitted by prospective clients in order to determine whether it can provide legal services, and prospective clients have a corresponding interest in having their enquiry properly considered. We carry out a Legitimate Interest Assessment in relation to this processing.

If you do not subsequently enter into a retainer with us, we will retain the personal data you have provided for a period of fifteen years from the date of your initial contact. This retention period is justified by the same legitimate interest that applies to concluded matters: any claim brought against GFL arising from the handling of your enquiry — including, for example, a claim relating to advice given at the enquiry stage or the handling of your personal data — may be brought on a date of knowledge basis, with a fifteen-year longstop under the Limitation Act 1980. We consider fifteen years to be a proportionate retention period having regard to that risk and to the minimal impact on the individual of retaining the data securely.

If your enquiry involves the disclosure of special category data — for example, information about an injury, medical condition or other sensitive personal circumstance — we will process that data on the basis that it is necessary for the establishment, exercise or defence of legal claims, in addition to our legitimate interest basis. Such data will be handled with the same level of care and security as special category data processed in connection with an active retainer.

You have the right to request deletion of personal data submitted at the enquiry stage. We will consider any such request carefully; however, we may decline to delete the data where we can demonstrate a compelling legitimate interest in retaining it, such as the need to defend a potential claim. We will write to you to explain our position if we decline a deletion request.

## **Processing of Personal Data under Your Retainer**

Where you instruct us to pursue a legal claim on your behalf, the contractual basis for our processing of your personal data is the retainer agreement between you and GFL — which may take the form of a Conditional Fee Agreement (CFA), a Damages-Based Agreement (DBA), or such other retainer as is agreed between us. We process your personal data because it is necessary to fulfil our obligations under that retainer.

We are unable to meet our contractual obligations to you without collecting and processing your personal data. If you are unable or unwilling to provide the personal data we require in order to pursue your claim, we may be unable to continue to act for you. In those circumstances, the terms of your retainer — including any provisions regarding fees — will apply. We will always explain our position to you in writing before taking any such step.

Where you contact us, make an enquiry, or instruct us in relation to the legal services that we offer — whether by telephone, email, via our websites, or by social media — we may contact you by post, telephone, email, direct messaging or SMS in relation to your enquiry or legal claim. You may opt out of receiving marketing communications from us at any time by notifying us verbally or in writing.

Where you apply for a position with GFL, we will process your personal data as part of the recruitment application process. Our lawful basis for this processing is our legitimate interest in fairly and effectively assessing candidates for employment (Article 6(1)(f) UK GDPR); we carry out a Legitimate Interest Assessment in relation to this processing. Where you voluntarily disclose special category data as part of your application — for example, information about a disability or medical condition relevant to a reasonable adjustment — we process that data on the basis that it is necessary for the purposes of carrying out our obligations, or exercising our rights, in the field of employment law (Article 9(2)(b) UK

GDPR and the employment condition in Schedule 1 to the DPA 2018), rather than on the basis of your consent.

### **Purposes for Processing Personal Data**

For legal claims and enquiries, the purpose for which your personal data is processed is the pursuance of your legal claim, or the consideration of the merits of representing you. We are unable to fulfil our contractual obligations to you without processing your personal data.

Personal data will also be held where you contact us in contemplation of pursuing a claim, whether or not the claim ultimately proceeds. We retain such data in accordance with our retention policy, in order to defend any legal claim pursued against us.

Where you engage with us via social media, we may contact you via direct messaging about the services that we offer. You have the right to opt out of receiving such messages.

In accordance with The Privacy and Electronic Communications (EC Directive) Regulations 2003, we may contact you by electronic means with regard to the services that we offer. You have the right to withdraw your consent and opt out of receiving electronic communications from us at any time. We also have a legitimate interest in contacting you by non-electronic means in relation to our services; you have the right to opt out of such communications at any time.

For applicants, the purpose of our processing is to consider your application for employment with GFL.

### **Lawful Basis for Processing Personal Data**

#### *Contract*

By entering into a retainer with us — whether a CFA, DBA or other agreed form of retainer — you have entered into a contract with us for legal services. We process your personal data because it is necessary to fulfil our obligations under that contract. The processing of personal data in pursuance of a claim is necessary and the retainer cannot be fulfilled in its absence.

#### *Legitimate Interest*

We have a legitimate interest in processing your personal data in pursuance of your claim. We also have a legitimate interest in retaining your personal data following the conclusion of your matter, in accordance with our retention policy, in order to defend any legal claim that may be pursued against us. Where we rely on legitimate interest as our lawful basis, we carry out a Legitimate Interest Assessment (LIA) to ensure that our interests do not override your rights and freedoms. Records of our LIAs are maintained and are available on request.

In certain circumstances, it may be appropriate to apply to the Court for an anonymity order, but that in itself would not circumvent the need to process your personal data as part of the claims process.

#### *Legal Obligation*

We are subject to a legal obligation, under UK financial sanctions law (the Sanctions and Anti-Money Laundering Act 2018 and the regulations made under it), to screen individuals against the UK sanctions lists and not to deal with funds or economic resources belonging to, or make them available to, a designated person. We process personal data as necessary to carry out that screening and to comply with any resulting reporting obligations.

#### *Direct Marketing*

For direct marketing, our lawful bases are consent (for electronic communications) and legitimate interest (for non-electronic communications). You have the right to opt out of both at any time.

#### *Recruitment*

For recruitment, our lawful basis is legitimate interest (Article 6(1)(f) UK GDPR) — we have a legitimate interest in assessing candidates fairly and effectively for potential employment, and we carry out a

Legitimate Interest Assessment in relation to this processing. Where you voluntarily disclose special category data as part of your application, we rely on the employment condition in Schedule 1 to the DPA 2018, together with Article 9(2)(b) UK GDPR, rather than on your consent.

### **The Categories of Personal Data Obtained**

For legal claims, the personal data we process will vary depending on the individual claim. In most cases, the standard personal data we require includes:

- Full legal name (including any alias)
- Address
- Date of birth
- Contact telephone numbers and/or email address

Certain claims will require the processing of additional personal data, which may include:

- National Insurance Number
- Benefits received
- Wage slips/earnings information
- Medical records
- Employment/personnel records
- Benefits records
- HMRC records
- Academic records
- Police reports
- Criminal records

In pursuance of your claim, we may need to process special category data — that is, more sensitive personal data such as medical records. Examples include information about an individual's:

- Race or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data (where used for identification purposes)
- Health
- Sex life or sexual orientation

Where we process special category data in pursuance of your claim, our condition for doing so is Article 9(2)(f) UK GDPR — that the processing is necessary for the establishment, exercise or defence of legal claims. Where we rely on a different Article 9 condition, an additional condition in Schedule 1 to the Data Protection Act 2018 may also be required; in those cases, the relevant condition is identified in the section dealing with that processing.

Data relating to criminal convictions, offences or allegations — including the police reports and criminal records referred to above — is not "special category data" under Article 9 UK GDPR. It is subject to a separate regime under Article 10 UK GDPR and Schedule 1 to the DPA 2018. Where we process this

data, we do so on the same lawful basis as other personal data processed in pursuance of your claim (see "Lawful Basis for Processing Personal Data" above), together with the Schedule 1 condition in paragraph 33 of Part 3 to Schedule 1 (Legal claims) — that the processing is necessary for the purpose of, or in connection with, legal proceedings (including prospective proceedings), is necessary for the purpose of obtaining legal advice, or is otherwise necessary for establishing, exercising or defending legal rights.

Processing of personal data will be restricted to what is reasonably necessary in pursuance of the claim. We take additional measures when processing sensitive data, including the use of recorded/special delivery mail and password-protected electronic documents.

In cases involving children or patients where a Litigation Friend is appointed, the collection and processing of personal data will include that of the Litigation Friend as well as the child or patient. Similarly, in cases pursued on behalf of an Estate, data relating to the Estate, the deceased and the Personal Representative will be processed.

### **Sending Personal Data to Us**

We use Transport Layer Security (TLS) to encrypt and protect email traffic. If your mail server does not support TLS, you should be aware that emails you send to us may not be protected in transit.

When you send personal data to us electronically, we recommend the use of secure email or file transfer platforms with encryption, or password-protected documents. We do not recommend sending personal data by post; if you do so, we recommend Special Delivery. Sending personal data by unencrypted email or ordinary post carries an inherent risk of loss or interception in transit; using one of the secure methods described above reduces that risk considerably.

### **The Sources of Personal Data**

The majority of personal data we collect will be provided by you directly. However, in some cases it will be necessary to obtain personal data from other sources, such as:

- Medical establishments (GP surgeries, hospitals, local health authorities)
- Medical agencies acting as data processors
- Employers (past and present)
- HMRC
- Department for Work and Pensions
- Compensation Recovery Unit
- Schools, colleges or universities
- Rehabilitation or treatment providers
- The opponent or their legal representative
- Other parties related to the case, such as witnesses, enquiry agents or previous solicitors' firms

### **The Categories of Recipients of the Personal Data**

In pursuance of a legal claim, various categories of recipient may receive your personal data. These may include, but are not limited to:

- The opponent and their insurer or legal representatives
- The Court
- A medical agency or medical expert
- Other expert witnesses

- A barrister
- Witnesses
- Department for Work and Pensions
- HMRC
- Employers (past and present)
- Partner law firms or law firms acting as our agents
- After the Event insurers or treatment providers
- Third party applications as necessary, such as WhatsApp, SharePoint, the High Court's CE-file system and the County Court's Damages Claims Portal.

From time to time, and where you have agreed to do so, we may communicate with you in relation to your matter via WhatsApp or other instant messaging platforms. Where we do so, personal data — which may include updates on your claim, documents, and in some cases special category data — will be processed on the infrastructure of the relevant third-party platform provider. WhatsApp is operated by Meta Platforms Inc., a US-based company; use of WhatsApp therefore involves the international transfer of personal data outside the United Kingdom. Meta processes such data under the UK Extension to the EU–US Data Privacy Framework (Meta is DPF-certified) and its own privacy terms. You are not obliged to communicate with us via WhatsApp or any other instant messaging platform. If you would prefer to communicate by a different means — such as telephone, post or email — please let us know and we will make alternative arrangements. Use of instant messaging platforms for client communications will always be by your agreement and at your election.

We use an electronic case management system (CMS) for the storage of case information. The CMS is provided by a third-party company (the CMSP). The CMSP has its own obligations under the DPA 2018 and UK GDPR and processes data only on our instructions.

GFL's IT infrastructure is hosted on a dedicated, sandboxed virtual server provided by a group IT services provider. That provider processes personal data only on GFL's instructions and is subject to a data processing agreement with GFL. Access to GFL's data environment is restricted and isolated from any other systems operated by the provider.

We store some personal data on servers owned, operated and maintained by third-party providers. Those providers have their own duties under the DPA 2018 and UK GDPR as data processors.

If your claim requires online submission via the Ministry of Justice's online portal, your personal data will be uploaded and communicated by the electronic portal as prescribed by the relevant pre-action protocols and court rules.

Our offices operate Closed Circuit Television (CCTV) cameras for the purpose of preventing and detecting crime and protecting staff and visitors, and we operate an audio recording system for telephone calls into and from the office for the purposes of dispute resolution, staff training and quality assurance. Our lawful basis for both is legitimate interests. CCTV footage is retained for six years, and call recordings are retained for fifteen years from the conclusion of the relevant case, save in either case where footage or a recording is required in connection with an ongoing investigation, complaint or legal claim, in which case it will be retained for as long as necessary for that purpose.

### **The Retention Periods for Personal Data**

Personal data will be retained by us for a minimum period of fifteen years following the conclusion of your matter (including the resolution of costs). Where a claim is lost or discontinued, the retention period runs from the date of final conclusion, including any appeal.

Personal data may be removed from our case management system after conclusion but will remain securely held for at least fifteen years before being securely erased, save for suppressed data as described below.

These retention periods also apply to any enquiry or proposed claim which, for whatever reason, we do not pursue. The fifteen-year period commences from the date of your initial contact with us.

For claims on behalf of minors, the retention period is fifteen years from the date of majority.

The fifteen-year retention period is justified by the nature of our business. Claims against us may be brought on a date of knowledge basis, extending beyond the standard six-year limitation period up to a fifteen-year longstop under the Limitation Act 1980. We consider fifteen years a proportionate balance between individual data rights and our legitimate interest in defending potential claims. A Legitimate Interest Assessment has been carried out in respect of this retention period.

Beyond the fifteen-year period, we may retain limited contact information — as "suppressed data" — for a maximum period of twenty-five years from the date of your initial contact with us. Where you have not opted out of contact, we retain this data in order to be able to contact you about our services. Where you have opted out of contact, we retain a minimal record of your details, marked so that you are not contacted again, in order to give effect to your opt-out and to avoid contacting you in future in error — a narrower purpose than, and distinct from, our original marketing purpose. Once the twenty-five-year outer limit is reached, we will securely delete this data.

For unsuccessful applicants, personal data will be retained for a period of six years following the conclusion of the recruitment process. This period reflects our legitimate interest in retaining sufficient records to identify whether an individual has previously applied to GFL, whether directly or via a recruitment agency, in order to assess and defend any claim for agency introduction fees that may arise. Six years mirrors the standard contractual limitation period under the Limitation Act 1980. Following the expiry of that period, recruitment data will be securely deleted.

## **Your Data Protection Rights**

### *Right of Access*

You have the right to access your personal data by making a subject access request (SAR), verbally or in writing. We will respond within one month, extendable by two months for complex or numerous requests. We will inform you of any extension within the first month. We may ask you to verify your identity before complying.

### *Right to Rectification*

You have the right to have inaccurate personal data corrected or incomplete data completed. We will respond within one month, extendable where requests are complex. We may charge a reasonable fee for requests that are manifestly unfounded or excessive.

### *Right to Erasure*

The right to erasure ('the right to be forgotten') is not absolute. It is not available where processing is necessary for the establishment, exercise or defence of legal claims. Personal data will be erased in accordance with our retention policy.

### *Right to Restrict Processing*

You may request that we restrict the processing of your personal data in certain circumstances — for example, where you contest its accuracy, or where processing is unlawful and you oppose erasure. Restriction may affect our ability to fulfil our obligations to you; we will write to you to explain if that is the case.

### *Right to Data Portability*

Where processing is based on consent or contract and is carried out by automated means, you have the right to receive your personal data in a structured, commonly used and machine-readable format, and to request that we transmit it to another controller. We will respond within one month.

### *Right to Object*

You have the right to object to processing based on legitimate interests or for direct marketing purposes. For direct marketing, the right is absolute. For other legitimate interest processing, we may continue if we can demonstrate compelling legitimate grounds that override your interests, or if processing is necessary for the establishment, exercise or defence of legal claims.

### *Rights in relation to Automated Decision-Making and Profiling*

Where you give your explicit consent, your eligibility for certain group data breach claims may be assessed by an automated scoring process, which can result in a decision about you — including a decision to close your claim — being taken without human involvement. This processing is described in full under "Use of Artificial Intelligence" below. Where such a decision is made about you, you have the right to obtain human intervention, to express your point of view, and to contest the decision, by contacting a member of staff as described in that section. Other than this automated eligibility scoring, our business activities do not currently involve automated individual decision-making or profiling that produces legal or similarly significant effects on you. If we intend to introduce further such processing, we will notify you in advance.

### *Right to Lodge a Complaint*

You have the right to lodge a complaint with the Information Commissioner's Office (ICO), the UK's supervisory authority for data protection. The ICO can be contacted at [www.ico.org.uk](http://www.ico.org.uk) or by telephone on 0303 123 1113.

## **International Transfers of Personal Data**

From time to time, we use third-party services that result in personal data being transferred outside the United Kingdom. Where the recipient is certified under the UK Extension to the EU–US Data Privacy Framework, we rely on that adequacy route; otherwise we put in place an International Data Transfer Agreement (IDTA) or the UK Addendum to the EU Standard Contractual Clauses, and, where required, carry out a Transfer Risk Assessment (TRA), to ensure that the level of protection afforded to personal data transferred internationally is not undermined by the laws or practices of the destination country.

Third-party services we currently use or may use that involve international transfers include:

- WhatsApp (Meta Platforms Inc.) — client communications where agreed and third party communications (US-based; transferred under the UK Extension to the EU–US Data Privacy Framework, Meta DPF-certified)
- Google Drive (Google LLC) and Microsoft OneDrive / SharePoint (Microsoft Corporation) — file storage (US-based; transferred under the UK Extension to the EU–US Data Privacy Framework)
- Claude (Anthropic, PBC) — AI-assisted drafting, research, document summarisation and claim triage (see "Use of Artificial Intelligence" below). Anthropic is a US-based provider and, under its current commercial service configuration, data may be processed in multiple geographic regions and stored in the United States. For UK GDPR-restricted transfers, Anthropic's data processing agreement incorporates the EU Standard Contractual Clauses together with the ICO's UK International Data Transfer Addendum.
- Microsoft Copilot (Microsoft Corporation) — AI-assisted drafting, research, document summarisation and claim triage (see "Use of Artificial Intelligence" below). Data is stored at rest in the United Kingdom; Microsoft's contractual framework nonetheless provides, for restricted

transfers, the Microsoft Products and Services Data Protection Addendum together with the relevant EU Standard Contractual Clauses and UK International Data Transfer Addendum.

The internet is a global medium and your information may pass through servers in various countries in transit. Transfers outside the UK are limited to those necessary for the establishment, exercise or defence of legal rights, obtaining legal advice, or in connection with legal proceedings.

### **Use of Artificial Intelligence**

Goldman Finch Limited uses artificial intelligence (AI) tools to assist with internal tasks including legal drafting, research and the summarisation of documents. This may involve the processing of your personal data — for example, where documents relating to your matter are drafted, reviewed or summarised with the assistance of an approved AI tool. Special category data (such as medical records) is only processed by an AI tool where a senior member of staff has given prior, documented authorisation on a per-matter basis. AI is used as an internal aid to support the work of our legal and administrative staff, and all outputs generated by AI tools are reviewed and approved by a qualified member of staff before being acted upon or relied upon.

Where third-party AI tools are used, they are provided under enterprise or commercial terms of service with appropriate contractual and data processing agreements in place, including terms which prevent your data from being used to train the provider's underlying AI models. We do not use personal, free, or consumer-tier AI accounts to process client or claimant personal data.

GFL uses AI tools to support the triage, evaluation and assessment of legal claims, including assisting a fee earner in considering the merits or value of your claim. Any such use of your personal data is carried out on the basis that it is necessary for the performance of your retainer with us, or, before a retainer is entered into, on the basis of our legitimate interest in evaluating your enquiry (as described above); and, where special category data is involved, on the basis that it is necessary for the establishment, exercise or defence of legal claims. You have the right to object to this processing, or to request human review of any AI-assisted output that affects you, in accordance with the rights set out above.

Other than the automated eligibility scoring described below, which only takes place with your explicit consent, GFL does not make any decisions about your matter solely by automated means. Any AI-assisted processing will involve human oversight, and you will retain the right to request that any significant decision affecting you is reviewed by a qualified member of staff. Where a decision or assessment about your matter has been informed by AI-assisted processing, we will identify this to you so that you are able to exercise that right.

Where you complete an online eligibility questionnaire in relation to a group data breach claim, some of the questions ask about the emotional or psychological impact the incident has had on you, and your answers to those questions constitute health data. Before you answer those questions, you will be asked to give explicit consent to that data being processed by an automated scoring process used to help determine whether your claim can proceed. The automated process considers your answers against the eligibility criteria for the claim type in question and generates a score; claims that score below the applicable threshold are closed, and claims that score at or above the threshold proceed to the next stage. We have carried out a Data Protection Impact Assessment in relation to this processing (reference GFL-DPIA-001). If you give your consent, your eligibility may be determined solely by that automated process, and, depending on your score, your claim may be closed without individual review by a member of staff. If your claim is closed on this basis, you have the right to ask a member of staff to review the questionnaire and the closure decision, to express your point of view on the decision, and to contest it. You may withdraw your consent at any time by contacting [dataprotection@goldmanfinch.com](mailto:dataprotection@goldmanfinch.com); withdrawal will not affect the lawfulness of processing carried out before you withdrew, and will not, of itself, reopen a claim that has already been closed on this basis — though you may still ask a member of staff to review that closure decision, as described above. If you do not wish to give this consent, or if you withdraw it, a member of our team will assess your eligibility

manually instead. Where your eligibility is assessed manually, we process the special category data in your questionnaire answers on the basis that it is necessary for the establishment, exercise or defence of legal claims (Article 9(2)(f) UK GDPR), rather than on the basis of your consent.

Whether your eligibility is assessed automatically or manually, the same criteria are applied. Manual assessment will take longer than automated assessment; we expect manual assessment to take no longer than a few weeks, though this may vary with the volume of claims we are handling at the time.

### **Accountability and Governance**

We take data protection seriously and are committed to compliance with our obligations as a data controller under the DPA 2018 and UK GDPR. We have in place proportionate processes, policies, records and logs for handling personal data, including records of processing activities and Legitimate Interest Assessments.

Should you wish to make a complaint in relation to the processing of your personal data, you may do so via our Complaints Handling Procedure. Complaints will be investigated by our Chief Legal Officer, and a full response will be provided within the timescales set out in that procedure.

You can contact us with any concerns about personal data at: [dataprotection@goldmanfinch.com](mailto:dataprotection@goldmanfinch.com)

Goldman Finch Limited is registered with the Information Commissioner's Office under registration number **ZB514670**. We implement technical and organisational measures to ensure and demonstrate compliance with our duties as a data controller. Those measures are risk-based, proportionate and reviewed regularly.

Goldman Finch Limited | Authorised and Regulated by the Solicitors Regulation Authority (SRA No. 816551)