Data Processing Agreement

CourtCorrect Ltd.

Document Name	Data Processing Agreement
Effective Date	13/04/2026
Policy Owner	CEO
Classification	Internal Use
Next Review Date	13/04/2027
ISMS Reference	Supporting Policy

CourtCorrect takes the privacy and security of your business data and personal information extremely seriously. This data processing agreement sets out how we, our partners and suppliers process and store your business data and personal information.

If you have any questions at all about how we handle your data, please don't hesitate to contact us at:

By email: hello@courtcorrect.com

By telephone: (+44) 0330 1332 411

By post: 33 Percy St, W1T 2DF, London, UK

1. Important Information and Who We Are

1.1. CourtCorrect Ltd is a company registered in England and Wales with company number 12117945 and its registered address at 33 Percy Street, W1T 2DF, London (collectively referred to as "CourtCorrect", "we", "us" or "our" in this Data Processing Agreement). CourtCorrect is the data processor responsible for your business data and personal information.

1.2. CourtCorrect is registered with the ICO with reference number ZB564422.

1.3. This data processing agreement aims to give you information on how CourtCorrect collects and processes your business data and personal information, including any data you may provide through our platform, when you sign up via our website, book or enquire about CourtCorrect.

1.4. CourtCorrect is not intended for children, and we do not knowingly collect data relating to children.

1.5. It is important that you read this data processing agreement together with any other terms we may provide on specific occasions when we are collecting or processing business data or personal information so that you are fully aware of how and why we are using your data. Should there be any conflict between any supplementary terms and this data processing agreement, this data processing agreement shall prevail with respect to all data processing matters.

2. Background

2.1. The Customer and CourtCorrect are in discussions regarding an agreement under which CourtCorrect will make available to the Customer a technology platform designed to assist in case and complaints management. In order for CourtCorrect to make the Services available, it is necessary for the Customer to share certain Business & Personal Data with CourtCorrect.

2.2. This Data Processing Agreement (the “Agreement”) sets out the terms, requirements and conditions on which CourtCorrect will process the Business & Personal Data when providing the Services to the Customer. This Agreement contains the mandatory clauses required by Article 28(3) of the UK GDPR for contracts between controllers and processors.

3. Agreed Terms

3.1. This Data Processing Agreement forms part of and is subject to the terms of the Terms & Conditions (“T&Cs”) between the parties. Capitalised terms not defined herein shall have the meanings given in the T&Cs.

3.2. The following definitions and rules of interpretation apply in this Agreement:

3.2.1. Business Purposes means the services to be provided by CourtCorrect to the Customer and any other purpose specifically identified.

3.2.2. Commissioner means the Information Commissioner (see Article 4(A3), UK GDPR and section 114, DPA 2018);

3.2.3. Data Protection Legislation means all applicable data protection and privacy legislation in force from time to time in the UK including without limitation the UK GDPR; the Data Protection Act 2018 (and regulations made thereunder) (DPA 2018); and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended;

3.2.4. EEA means the European Economic Area;

3.2.5. Records has the meaning given to it in Clause 14;

3.2.6. Term means this Agreement’s term as defined in Clause 12;

3.2.7. UK GDPR has the meaning given to it in section 3(10) (as supplemented by section 205(4)) of the DPA 2018;

3.2.8. Controller, Processor, Data Subject, Personal Data, Personal Data Breach and Processing: have the meanings given to them in the Data Protection Legislation.

3.3. The Annexes form part of this Agreement and will have effect as if set out in full in the body of this Agreement. Any reference to this Agreement includes the Annexes.

3.4. A reference to writing or written includes email but not fax.

3.5. The Customer and CourtCorrect agree and acknowledge that for the purpose of the Data Protection Legislation:

3.5.1. the Customer is the Controller, and CourtCorrect is the Processor.

3.5.2. the Customer retains control of the Business & Personal Data and remains responsible for its compliance obligations under the Data Protection Legislation, including but not limited to,

providing any required notices and obtaining any required consents, and for the written processing instructions it gives to CourtCorrect.

3.5.3. this agreement describes the subject matter, duration, nature and purpose of the processing and the Business & Personal Data categories and Data Subject types in respect of which CourtCorrect may process the Business & Personal Data to fulfil the Business Purposes.

3.5.4. If CourtCorrect processes Personal Data for purposes not authorised by the Customer's documented instructions or this Agreement, CourtCorrect shall be considered a Controller in respect of that processing and shall bear sole responsibility for its compliance with the Data Protection Legislation in relation to such processing, in accordance with Article 28(10) of the UK GDPR.

4. Customer's Responsibilities

4.1. The Customer shall ensure that all Personal Data and Business Data shared with CourtCorrect have been collected, processed and disclosed in accordance with applicable Data Protection Legislation, including ensuring that any required notices have been given to Data Subjects and any necessary consents or lawful basis for processing have been obtained.

4.2. The Customer represents and warrants that all Personal Data provided to CourtCorrect are accurate, complete and up to date to the best of its knowledge and belief.

4.3. The Customer acknowledges that CourtCorrect, as a data processor, relies entirely on the Customer's instructions and representations in relation to the lawfulness, accuracy and completeness of the Personal Data. CourtCorrect shall not be responsible for any non-compliance arising from or connected to the Customer's failure to comply with its obligations as a data controller under the Data Protection Legislation.

4.4. The Customer shall promptly notify CourtCorrect of any changes to the lawful basis or scope of processing, or any event that may impact the lawfulness of processing under this Agreement.

4.5. The Customer shall indemnify and hold harmless CourtCorrect against all claims, liabilities, losses, damages, costs and expenses (including reasonable legal fees) arising from or in connection with: (a) the Customer's breach of its obligations as a data controller under the Data Protection Legislation; (b) the Customer's provision of unlawful, inaccurate, or excessive Personal Data to CourtCorrect; (c) the Customer's failure to obtain valid consent or establish a lawful basis for processing where required; or (d) any processing instruction given by the Customer that infringes the Data Protection Legislation. This indemnity shall not apply to the extent that the relevant claim arises from CourtCorrect's breach of this Agreement or negligence.

5. CourtCorrect's Obligations

5.1. CourtCorrect will only process the Business & Personal Data to the extent, and in such a manner, as is necessary for the Business Purposes in accordance with the Customer's written instructions. CourtCorrect will not process the Business & Personal Data for any other purpose or in a way that does not comply with this Agreement or the Data Protection Legislation. CourtCorrect must promptly notify the Customer if, in its opinion, the Customer's instructions do not comply with the Data Protection Legislation.

5.2. Where the Customer elects to enable CourtCorrect's AI-assisted features, the Customer authorises CourtCorrect to use Customer Data, including Personal Data processed on the

Customer's behalf, solely for the purpose of model optimisation, quality improvement, and performance tuning of Customer-specific AI models. Such processing shall be carried out in accordance with the Customer's documented instructions, shall not result in the commingling of Customer Data with data of any other customer, and shall not be used to train or improve any models for the benefit of third parties. CourtCorrect shall apply appropriate technical and organisational measures, including isolation of datasets, to ensure that Customer Data used for such optimisation remains segregated. For the avoidance of doubt: (a) all intellectual property rights in AI models, algorithms, weights, and outputs generated or improved through such optimisation shall remain the property of CourtCorrect; (b) aggregated, anonymised, or statistical insights derived from the optimisation process that do not constitute Personal Data may be retained and used by CourtCorrect; and (c) if the Customer subsequently withdraws authorisation for AI-assisted features, CourtCorrect shall cease further processing of new Customer Data for optimisation purposes but shall not be required to retrain, modify, or delete models that have already been optimised using data processed during the authorised period.

5.3. CourtCorrect must comply promptly with any Customer written instructions requiring CourtCorrect to amend, transfer, delete or otherwise process the Business & Personal Data, or to stop, mitigate or remedy any unauthorised processing.

5.4. CourtCorrect will maintain the confidentiality of the Business & Personal Data and will not disclose the Business & Personal Data to third parties unless the Customer or this Agreement specifically authorises the disclosure, or as required by domestic law, court or regulator (including the Commissioner). If a domestic law, court or regulator (including the Commissioner) requires CourtCorrect to process or disclose the Business & Personal Data to a third-party, CourtCorrect must first inform the Customer of such legal or regulatory requirement and give the Customer an opportunity to object or challenge the requirement, unless the domestic law prohibits the giving of such notice.

5.5. CourtCorrect will reasonably assist the Customer, at no additional cost to the Customer, with meeting the Customer's compliance obligations under the Data Protection Legislation, taking into account the nature of CourtCorrect's processing and the information available to CourtCorrect, including in relation to Data Subject rights, reporting to and consulting with the Commissioner under the Data Protection Legislation.

5.6. CourtCorrect shall, taking into account the nature of the processing and the information available to CourtCorrect, provide the Customer with such information about CourtCorrect's processing activities as is reasonably necessary for the Customer to carry out data protection impact assessments pursuant to Article 35 of the UK GDPR and, where required, to consult with the Commissioner pursuant to Article 36 of the UK GDPR.

5.7. CourtCorrect must notify the Customer promptly of any changes to the Data Protection Legislation that may reasonably be interpreted as adversely affecting CourtCorrect's performance of the Terms and Conditions or this Agreement.

6. CourtCorrect's Employees

6.1. CourtCorrect will ensure that all of its employees:

6.1.1. are informed of the confidential nature of the Business & Personal Data and are bound by written confidentiality obligations and use restrictions in respect of the Business & Personal Data;

6.1.2. have undertaken training on the Data Protection Legislation and how it relates to their handling of the Business & Personal Data and how it applies to their particular duties; and

6.1.3. are aware both of CourtCorrect's duties and their personal duties and obligations under the Data Protection Legislation and this Agreement.

7. Security

7.1. CourtCorrect must at all times implement appropriate technical and organisational measures against accidental, unauthorised or unlawful processing, access, copying, modification, reproduction, display or distribution of the Business & Personal Data, and against accidental or unlawful loss, destruction, alteration, disclosure or damage of the Business & Personal Data including, but not limited to, the security measures set out in this agreement.

7.2. CourtCorrect must implement such measures to ensure a level of security appropriate to the risk involved, including as appropriate:

7.2.1. the pseudonymisation and encryption of personal data;

7.2.2. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

7.2.3. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and

7.2.4. a process for regularly testing, assessing and evaluating the effectiveness of the security measures.

8. Personal Data Breach

8.1. CourtCorrect will immediately and in any event without undue delay notify the Customer in writing if it becomes aware of:

8.1.1. the loss, unintended destruction or damage, corruption, or unusability of part or all of the Personal Data;

8.1.2. any accidental, unauthorised or unlawful processing of the Personal Data; or

8.1.3. any Personal Data Breach.

8.2. Where CourtCorrect becomes aware of any of the above, it will, without undue delay, also provide the Customer with the following written information:

8.2.1. description of the nature of the breach, including the categories of in-scope Personal Data and approximate number of both Data Subjects and the Personal Data records concerned;

8.2.2. the likely consequences; and

8.2.3. a description of the measures taken or proposed to be taken to address the breach, including measures to mitigate its possible adverse effects.

8.3. Immediately following any accidental, unauthorised or unlawful Personal Data processing or Personal Data Breach, the parties will co-ordinate with each other to investigate the matter. Further, CourtCorrect will reasonably co-operate with the Customer at no additional cost to the Customer, in the Customer's handling of the matter, including but not limited to:

8.3.1. assisting with any investigation;

8.3.2. providing the Customer with physical access to any facilities and operations affected;

8.3.3. facilitating interviews with CourtCorrect's employees and others involved in the matter including, but not limited to, its officers and directors;

8.3.4. making available all relevant records, logs, files, data reporting and other materials required to comply with all Data Protection Legislation or as otherwise reasonably required by the Customer; and

8.3.5. taking reasonable and prompt steps to mitigate the effects and to minimise any damage resulting from the Personal Data Breach or accidental, unauthorised or unlawful Personal Data processing.

8.4. CourtCorrect will not inform any third-party of any accidental, unauthorised or unlawful processing of all or part of the Personal Data and/or a Personal Data Breach without first obtaining the Customer's written consent, except when required to do so by domestic law.

8.5. CourtCorrect agrees that the Customer has the sole right to determine:

8.5.1. whether to provide notice of the accidental, unauthorised or unlawful processing and/or the Personal Data Breach to any Data Subjects, the Commissioner, other in-scope regulators, law enforcement agencies or others, as required by law or regulation, including the contents and delivery method of the notice; and

8.5.2. whether to offer any type of remedy to affected Data Subjects, including the nature and extent of such remedy.

8.6. CourtCorrect will cover all reasonable expenses associated with the performance of these obligations unless the matter arose from the Customer's specific written instructions, negligence, wilful default or breach of this Agreement, in which case the Customer will cover all reasonable expenses.

8.7. CourtCorrect will also reimburse the Customer for actual reasonable expenses that the Customer incurs when responding to an incident of accidental, unauthorised or unlawful processing and/or a Personal Data Breach to the extent that CourtCorrect caused such incident, including all costs of notice and any remedy.

9. Cross-Border Transfers of Personal Data

9.1. CourtCorrect and its subprocessors may process or transfer Personal Data outside the United Kingdom ("UK") and the European Economic Area ("EEA") where such transfer is necessary for the provision of the Services, provided that such transfers are carried out in accordance with applicable Data Protection Legislation.

9.2. Where Personal Data is transferred to a country or territory that is subject to an adequacy decision by the UK Government or the European Commission — including the UK–US Data Bridge (the UK extension to the EU–US Data Privacy Framework) — such transfers shall be permitted without additional authorisation.

9.3. Where Personal Data is transferred to a country or territory not subject to an adequacy decision, CourtCorrect shall ensure that appropriate safeguards are implemented in accordance with Chapter V of the UK GDPR and, where applicable, Chapter V of the EU GDPR, which may include, as applicable: (a) the use of Standard Contractual Clauses approved by the UK

Government or European Commission (and any applicable UK Addendum); or (b) International Data Transfer Agreement; or (c) Binding Corporate Rules approved by a competent supervisory authority; or (d) any other legally recognised transfer mechanism that ensures an essentially equivalent level of protection for the Personal Data.

9.4. Where a proposed transfer cannot be legitimised under paragraphs (9.2) or (9.3) above, CourtCorrect shall obtain the Customer's specific prior written consent before any such transfer takes place.

9.5. CourtCorrect shall implement appropriate technical and organisational measures to ensure that any such transfers are conducted securely and in compliance with Data Protection Legislation.

9.6. For the avoidance of doubt, the existence of cross-border transfers of Personal Data under this Clause 9 shall not, in itself, constitute a breach of this Agreement, provided that such transfers are made in accordance with the safeguards set out above.

10. Subprocessors

10.1. The Customer grants CourtCorrect a general prior authorisation to engage subprocessors to process Personal Data on its behalf for the purposes of providing the Services under this Agreement, provided that:

(a) CourtCorrect notifies the Customer in advance of any intended addition or replacement of subprocessors that will result in a new or materially different processing of Personal Data, or any material change to a transfer mechanism that may materially affect the level of protection afforded to Personal Data, thereby giving the Customer the opportunity to object on reasonable grounds related to data protection;

(b) CourtCorrect ensures that appropriate safeguards are in place with each subprocessor, which may include written data processing agreements, the subprocessor's standard contractual terms, adherence to recognised security or data protection standards, or a combination of such measures, in each case sufficient to ensure an appropriate level of protection for Personal Data;

(c) CourtCorrect maintains an up-to-date list of approved subprocessors and their processing locations in Annex A to this Agreement, which shall be updated to reflect any additions or replacements made in accordance with this Clause 10;

(d) upon the Customer's reasonable written request, CourtCorrect will provide information regarding the data protection safeguards applicable to any subprocessor, which may include: (i) directing the Customer to the subprocessor's publicly available terms, certifications, or security documentation; and (ii) providing a summary of the relevant findings from CourtCorrect's own risk assessment of that subprocessor. For the avoidance of doubt, CourtCorrect shall not be required to disclose any third-party documentation that is subject to confidentiality obligations;

(e) each subprocessor's engagement shall automatically terminate upon the termination or expiry of this Agreement for any reason.

10.2. The subprocessors approved as of the commencement of this Agreement are listed in Annex A. CourtCorrect shall maintain an up-to-date record of all current subprocessors, including their legal name, location, and a summary of their processing activities. Details of any

new or replacement subprocessors engaged after the commencement of this Agreement shall be made available to the Customer upon request.

10.3. In relation to Clause 10.1(a), the Customer may object to the appointment of a new subprocessor or to any material change to a transfer mechanism on reasonable and substantiated data protection grounds within fourteen (14) days of receiving notice.

10.4. In the event of an objection, CourtCorrect shall, at its sole discretion: (i) use reasonable efforts to propose an alternative subprocessor; (ii) take reasonable steps to address the Customer's concerns; or (iii) where neither of the foregoing is feasible, permit the Customer to use the Platform without the affected Services upon written notice, solely with respect to the relevant processing activity, without liability to either party and without any obligation on CourtCorrect to refund or reimburse any fees already paid.

10.5. Where an objection under Clause 10.3 cannot be resolved in accordance with Clause 10.4 within thirty (30) days of the Customer's objection notice, and the Customer can reasonably demonstrate that the proposed subprocessor change would materially reduce the level of data protection afforded to the Customer's Personal Data, the Customer may terminate the affected Service component (but not the entire Agreement) upon thirty (30) days' written notice, without penalty to either party. For the avoidance of doubt, this termination right applies only to the specific Service component affected by the disputed subprocessor change and does not entitle the Customer to terminate the Agreement as a whole or to receive a refund of fees attributable to unaffected Services.

10.6. CourtCorrect shall remain liable for the acts and omissions of its subprocessors to the same extent as if CourtCorrect had performed the relevant processing itself, in accordance with Article 28(4) of the UK GDPR. However, CourtCorrect's liability under this Clause shall not extend to losses arising from a subprocessor's acts or omissions where CourtCorrect can demonstrate that: (a) it exercised reasonable due diligence in the selection and appointment of the subprocessor; (b) it ensured that appropriate data protection safeguards were in place with the subprocessor in accordance with Clause 10.1(b); and (c) the loss arose from the subprocessor's breach of those obligations and not from any failure by CourtCorrect to oversee or manage the subprocessor.

10.7. For the avoidance of doubt, the engagement of subprocessors in accordance with this clause and any lawful cross-border transfer of Personal Data under this clause shall not, in themselves, constitute a breach of this Agreement or the Data Protection Legislation, provided that the requirements of these clauses have been met.

11. Complaints, Data Subject Requests and Third-Party Rights

11.1. CourtCorrect must, at no additional cost to the Customer, take such technical and organisational measures as may be appropriate, and promptly provide such information to the Customer as the Customer may reasonably require, to enable the Customer to comply with:

11.1.1. the rights of Data Subjects under the Data Protection Legislation, including, but not limited to, subject access rights, the rights to rectify, port and erase personal data, object to the processing and automated processing of personal data, and restrict the processing of personal data; and

11.1.2. information or assessment notices served on the Customer by the Commissioner under the Data Protection Legislation.

11.2. CourtCorrect must notify the Customer in writing if it receives any complaint, notice or communication that relates directly or indirectly to the processing of the Personal Data or to either party's compliance with the Data Protection Legislation.

11.3. CourtCorrect must notify the Customer without undue delay and in any event within forty-eight (48) hours if it receives a request from a Data Subject for access to their Personal Data or to exercise any of their other rights under the Data Protection Legislation.

11.4. CourtCorrect will give the Customer, at no additional cost to the Customer, its full co-operation and assistance in responding to any complaint, notice, communication or Data Subject request.

11.5. CourtCorrect must not disclose the Personal Data to any Data Subject or to a third-party other than in accordance with the Customer's written instructions, or as required by domestic law. If the Customer's written instructions directly contradict domestic law, domestic law will prevail.

12. Term and Termination

12.1. This Agreement will remain in full force and effect so long as CourtCorrect retains any of the Personal Data related to the Terms and Conditions in its possession or control.

13. Data Return and Destruction

13.1. At the Customer's request, CourtCorrect will give the Customer, or a third-party nominated in writing by the Customer, a copy of or access to all or part of the Personal Data associated with the Customer's account that is in CourtCorrect's possession or control in the format and on the media reasonably specified by the Customer.

13.2. Upon termination or expiry of this Agreement, or upon the Customer's written request, CourtCorrect shall, without undue delay, delete or anonymise all Personal Data and Business Data in its possession or control that were processed on behalf of the Customer, unless retention of such data is required by applicable law, regulation, government or regulatory body, or for legitimate business, audit, or compliance purposes.

13.3. Where retention is required, CourtCorrect shall inform the Customer in writing of the legal basis for such retention, materials or Personal Data that it must retain, and the expected timeline for deletion or anonymisation once the retention requirement ceases.

13.4. Upon request by the Customer, CourtCorrect will certify in writing to the Customer that it has deleted or destroyed the Personal Data within 5 working days after it completes the deletion or destruction.

13.5. Notwithstanding the foregoing, CourtCorrect shall not be obliged to delete or return data that has been aggregated, pseudonymised, or anonymised in such manner that it no longer constitutes Personal Data under the Data Protection Legislation.

13.6. Nothing in this clause shall prevent CourtCorrect from retaining backup copies of data for a limited period in accordance with its standard data retention and disaster recovery policies, provided that such copies remain subject to appropriate technical and organisational safeguards and are deleted in the ordinary course of business.

14. Records

14.1. CourtCorrect will keep detailed, accurate and up-to-date written records regarding any processing of the Personal Data, including but not limited to, the access, control and security of the Personal Data, approved subprocessors, the processing purposes, categories of processing, international transfers of Personal Data, and a general description of the technical and organisational security measures referred to in this agreement. These records shall satisfy the requirements of Article 30(2) of the UK GDPR and shall include, at a minimum: (a) the name and contact details of CourtCorrect and, where applicable, the Customer; (b) the categories of processing carried out on behalf of the Customer; (c) where applicable, details of transfers of Personal Data to a third country or international organisation, including the identification of that third country or international organisation and the documentation of appropriate safeguards; and (d) where possible, a general description of the technical and organisational security measures.

14.2. CourtCorrect will ensure that the Records are sufficient to enable the Customer to verify CourtCorrect's compliance with its obligations under this Agreement and the Data Protection Legislation and CourtCorrect will provide the Customer with copies of the Records upon request.

14.3. The Customer and CourtCorrect must review the information listed in the Annexes to this Agreement at least once a year to confirm its current accuracy and update it when required to reflect current practices.

15. Audit

15.1. The Customer may, upon giving at least thirty (30) days' prior written notice, conduct a security review or audit CourtCorrect's compliance with this Agreement in respect of the processing of Customer Personal Data. CourtCorrect shall provide reasonable assistance to the Customer with any request regarding subprocessors or third parties that act as processors in connection with the Services, subject to CourtCorrect's confidentiality obligations and the rights of its other customers and suppliers. The Customer shall carry out any inspection in such a way as to minimise disruption to CourtCorrect.

15.2. CourtCorrect shall, where an audit identifies any material non-compliance with this Agreement or applicable Data Protection Legislation in respect of the processing of Customer Personal Data, take appropriate corrective actions within a reasonable period of time, taking into account the nature and severity of the finding. CourtCorrect shall not be obliged to implement any specific remediation measure proposed by the Customer where CourtCorrect reasonably considers such measure to be disproportionate, commercially unreasonable or technically infeasible.

15.3. Audits or inspections under this Agreement shall be limited to one (1) per calendar year, except where a further audit is reasonably required following a material Personal Data Breach. The Customer shall provide at least thirty (30) days' prior written notice of any audit, which shall be conducted during CourtCorrect's normal business hours and in a manner that does not unreasonably disrupt or interfere with CourtCorrect's operations. The Customer shall bear its own costs in connection with any such audit and shall reimburse CourtCorrect for reasonable and demonstrable material time or resources expended to facilitate the audit. CourtCorrect may, at its discretion, satisfy the Customer's audit rights (in whole or in part) by providing up-to-date third-party audit reports, certifications, summaries of penetration tests or other industry-standard attestations demonstrating the effectiveness of its technical and organisational measures.

16. Warranties

16.1. CourtCorrect warrants that:

16.1.1. its employees, subprocessors, agents and any other person or persons accessing the Personal Data on its behalf are reliable and trustworthy and have received the appropriate training on the Data Protection Legislation;

16.1.2. it and anyone operating on its behalf shall use reasonable endeavours to process the Personal Data in compliance with the Data Protection Legislation and other laws, enactments, regulations, orders, standards and other similar instruments;

16.1.3. it has no reason to believe that the Data Protection Legislation materially restricts or prevents it from providing any of the Services; and

16.1.4. considering the current technology environment and implementation costs, it will implement and maintain appropriate technical and organisational measures to prevent the accidental, unauthorised or unlawful processing of Personal Data and the loss or damage to the Personal Data, and ensure a level of security appropriate to: (a) the harm that might result from such accidental, unauthorised or unlawful processing and loss or damage; (b) the nature of the Personal Data protected; and (c) compliance with all applicable Data Protection Legislation and with its information and security policies, including the security measures required in this agreement.

16.2. The Customer warrants and represents that CourtCorrect's commercially reasonable use of the Personal Data for the Business Purposes and as specifically instructed by the Customer will comply with the Data Protection Legislation.

17. Limitation of Liability

17.1. The liability of each party arising under or in connection with this Agreement (including in respect of any data protection claims, indemnities, or breaches of data processing obligations) shall be subject to the limitations and exclusions of liability set out in the Terms & Conditions between the parties. For the avoidance of doubt, the limitations of liability in the Terms & Conditions shall apply to claims arising under this Agreement to the same extent as claims arising under the Terms & Conditions generally.

17.2. Nothing in this Agreement shall limit either party's liability for: (a) fraud or fraudulent misrepresentation; (b) death or personal injury caused by its negligence; or (c) any other liability that cannot be limited or excluded by applicable law.

18. Notice

18.1. Any notice given to a party under or in connection with this Agreement must be in writing and delivered to:

- For the Customer: [•]
- For CourtCorrect: Ludwig Konrad Bull, CEO & Founder – ludwig@courtcorrect.com

19. Version History

Version	Date	Author	Description	Approved by
1.0	01/05/2023	L. Langridge	Initial policy creation.	L. Bull
2.0	27/04/2024	L. Langridge	No changes made.	L. Bull
3.0	26/04/2025	E. Marin	Annual review.	L. Bull
4.0	01/08/2025	E. Marin	Review and update of sub-processors' list.	L. Bull
5.0	01/12/2025	A. Naiko	Review and update of sub-processors' list.	L. Bull
6.0	13/04/2026	A. Naiko	Added DPIA assistance clause, reciprocal customer indemnity, sub-processor liability with due diligence standard, AI optimisation IP protections, Article 30(2) records reference, DSAR forwarding tightened to 48 hours, access revocation aligned to 48 hours, sub-processor notification timeline made explicit (14 days), customer termination right for unresolvable sub-processor objections	L. Bull

ANNEX A — PERSONAL DATA PROCESSING PURPOSES AND DETAILS

Processing by CourtCorrect

1. Scope

CourtCorrect's employees, its systems and all Customer and Complainant personal data in whatever form it is held.

2. Nature

CourtCorrect is permitted to collect, process, sort, save, transfer, restrict and delete data only to the extent necessary to provide the Services, including AI-assisted case handling and complaints management functionality.

3. Purpose of Processing

CourtCorrect processes Personal Data on behalf of the Customer for the purpose of providing the Services under the Terms & Conditions, including case handling, complaints management, AI-assisted analysis, and reporting. The Customer, as Controller, is responsible for determining the lawful basis for such processing in accordance with the Data Protection Legislation.

4. Duration of the Processing

The processing will last no longer than required by CourtCorrect in order to fulfil its obligations under the Terms & Conditions, or for such a period of time as is reasonably needed to provide the Customer with the Services, subject to the data return and destruction provisions in Clause 13.

Types of Personal Data

CourtCorrect will process the following types of data on behalf of the Customer:

- Names
- Personal contact details (customer and third party)
- Details of the case
- Date of birth
- Vulnerabilities
- Other evidence that may form part of the case

Categories of Data Subject

- Customers, customers' staff members, complainants, and third-party suppliers.

Subprocessors

Subprocessor	Description	Processing Location
OpenAI	Provides large language model (LLM) services which CourtCorrect uses to deliver certain AI-assisted functionality. CourtCorrect processes limited Customer	European Union, United States

Subprocessor	Description	Processing Location
	Data through OpenAI's Business API solely for the purpose of generating model outputs in accordance with the Customer's documented instructions. OpenAI processes such data only as CourtCorrect's sub-processor. Customer Data processed via the Business API is not used by OpenAI for model training, benchmarking, or product improvement. OpenAI permanently deletes data submitted through the API within 30 days, unless a shorter period applies under CourtCorrect's configuration.	(depending on customer configuration)
OVHCloud	Provides cloud hosting and storage services for the CourtCorrect platform. OVHCloud acts solely as CourtCorrect's sub-processor and provides ISO- and SOC-certified security and availability controls. OVHCloud does not access Customer Data.	Frankfurt, Germany and Erith, United Kingdom
Amazon Web Services (AWS)	Provides cloud hosting and infrastructure services used by CourtCorrect for the operation of its platform, including the hosting of frontend and backend applications, as well as the deployment of custom and fine-tuned large language models. AWS is also used for the storage of Customer Data uploaded to the CourtCorrect platform. All Customer Data stored by CourtCorrect in AWS is hosted in AWS's data centres located in Frankfurt, Germany and London, United Kingdom. AWS acts strictly as a processor and processes Customer Data only on CourtCorrect's documented instructions.	Frankfurt, Germany and London, United Kingdom
Qdrant	Provides vector search database services to enable efficient similarity search and management of high-dimensional data, supporting use cases like recommendation systems and semantic search.	Frankfurt, Germany
Hotjar	Provides analytics platform services for insights into user behaviour on the CourtCorrect website and application. Hotjar anonymises user data and provides controls for user consent.	Ireland, European Union
LiveChat	Provides customer support communication tool used by CourtCorrect solely for real-time assistance to authorised users. LiveChat does not have access to Case Data, operational data, or other Customer Data processed within the CourtCorrect solution. Personal data processed by LiveChat is limited to support-related information voluntarily provided by authorised users during a support interaction.	United States
AssemblyAI	Provides speech-to-text transcription services enabling the CourtCorrect platform to process audio data. AssemblyAI does not store any audio data after processing and employs end-to-end encryption and strict access controls.	Ireland, European Union
Google Cloud	Provides cloud computing services used by CourtCorrect for advanced analytics on cases. Google Cloud's models	London, United Kingdom

Subprocessor	Description	Processing Location
	process but do not permanently store data, including case file information containing personal data.	
LlamaIndex	Provides document-processing and data-structuring services used to support LLM functionality, including parsing, ingestion, and transformation of complex or unstructured documents into structured, machine-readable data. LlamaIndex does not use Customer Data for model training.	European Union
LangChain	Enables CourtCorrect to support the development, testing, deployment, and management of its large language models. Monitors inputs and logs outputs in a dedicated database in the European Union.	European Union
Sentry	Supports CourtCorrect with monitoring and error tracking of the platform, collecting information about potential errors, crashes, and performance problems across backend and frontend systems.	European Union
Redis	Provides high-performance storage and processing capabilities to support AI-driven features on the CourtCorrect platform, including rapid message handling and computation.	European Union

ANNEX B — SECURITY MEASURES

Technical and Organisational Measures

1. Information Security Commitments

CourtCorrect is committed to maintaining the confidentiality, integrity and availability of all data it accesses, processes or stores and to implementing appropriate technical and organisational measures consistent with applicable Data Protection Legislation and Good Industry Practice.

2. Information Security Policy and Governance

(a) CourtCorrect shall ensure that the subject of information security and its importance to CourtCorrect's business is represented at a senior level within CourtCorrect's organisation and that a formal strategy for information security management has been approved by management.

(b) A documented and approved information security policy shall be maintained. This policy must be communicated to CourtCorrect's personnel, contractors and all their third parties with access to Personal Data or CourtCorrect's information systems.

(c) The information security policy shall be enforced across the organisation, reviewed on at least an annual basis or when a significant change has occurred that necessitates the modification of policy. CourtCorrect shall ensure that there is a formal disciplinary process for breaches of this policy.

(d) CourtCorrect shall develop, implement, operate, maintain and continuously improve an Information Security Management System ("ISMS") which is in alignment to Good Industry Practice and ISO 27001.

3. Awareness and Training

(a) CourtCorrect shall provide all employees who have access to Personal Data with clear roles and responsibilities pertaining to information security and data protection.

(b) CourtCorrect will provide employees with specific information security training detailing good security practices on at least an annual basis. Training shall reflect CourtCorrect's internal policies, relevant legal obligations and security expectations.

4. Access Control

(a) CourtCorrect shall ensure that access control to information systems that host, access or process Personal Data is maintained to only those who need access.

(b) Each user shall authenticate using a unique username and strong password before being granted access to applications, computers and network devices. The account provided to employees must have permissions that are appropriate to the role they carry out.

(c) The access that has been provided to employees shall be reviewed on a quarterly basis to ensure that access granted is required.

(d) Access provided shall be revoked without undue delay and in no event later than forty-eight (48) hours after an employee leaves the organisation or no longer has a requirement to access the information system.

5. Secure Configuration and Vulnerability Management

(a) All external connections to CourtCorrect's networks and applications shall comply with CourtCorrect's security configuration standards.

(b) All network traffic from external sources must be routed through a firewall before being allowed access to CourtCorrect's network. CourtCorrect shall maintain appropriate perimeter security controls consistent with Good Industry Practice.

(c) Wireless access to CourtCorrect information systems shall follow CourtCorrect's internal network security standards.

(d) CourtCorrect shall ensure that its computers and network devices are securely configured.

(e) CourtCorrect shall ensure that all software running on computers and network devices is properly licensed, vendor-supported, and kept fully up to date, with all relevant security patches and updates installed in a timely manner to mitigate known vulnerabilities.

6. Malware Protection

(a) CourtCorrect shall ensure that information, applications and computers within the organisation's internal networks are protected against unauthorised access and disclosure from the internet, using boundary firewalls, internet gateways or equivalent network devices. CourtCorrect shall implement robust malware protection on exposed computers to reduce the risk posed by malicious code and harmful content. The malware protection software shall be implemented across relevant systems and shall be kept up-to-date.

7. Monitoring

(a) CourtCorrect shall deploy intrusion detection tools in CourtCorrect IT systems to identify suspected or actual attacks and respond in accordance with its security incident management process.

(b) Logs of all security events will be maintained, such as those that have the potential to impact the service provided to the Customer and that may assist in the identification or investigation of security incidents and breaches of access in relation to CourtCorrect's systems.

8. Information System Development

(a) Activities must be carried out in accordance with a documented system development methodology which shall be shared with Customer upon request. Information security requirements shall be considered from the onset of systems design.

(b) Quality assurance checks and reviews shall be included in the development lifecycle. CourtCorrect shall ensure that all elements of CourtCorrect systems are tested at all stages of the systems development lifecycle before the system is promoted to the live environment.

(c) Changes to information processing systems must be controlled by the use of a formal change control procedure. This procedure shall ensure that: a formal process of documentation is maintained; testing is conducted; quality control is ensured; any change in service is introduced; and the ability to regress is enabled.

(d) Where CourtCorrect outsources development to a third party, CourtCorrect must ensure that the standards made in this Agreement are adhered to. CourtCorrect's third party must also be subject to CourtCorrect's third party assurance process.

(e) System development activities shall be performed in an IT environment isolated and separate from the production environment. CourtCorrect shall ensure that live Customer data (including Personally Identifiable Data) will not be used within the test environment.