

# Changefirst Ltd

## Data Processing Agreement

Last Modified: June 17, 2022

This agreement is inclusive of the Changefirst Data Processing terms, description of the processing (Sections 7-11) and the technical and organisational security measures (Sections 12-21). It is to be read in conjunction with the Changefirst Master Agreement.

The scope and duration as well as the extent and nature of the collection, processing and user of personal data under this Policy shall be as defined in the Agreement. The term of this agreement corresponds to the duration of the Agreement.

### DEFINITIONS

**Client Personal Data** means the personal data processed by Changefirst on your behalf during providing Services to you.

**Data Protection Legislation** means the UK Data Protection Act 2018 and any legislation and/or regulation implementing or made pursuant to them, or which amends, replaces, re-enacts or consolidates it;

**Data processor, data subject, personal data, processing and appropriate technical and organisational measures** shall be interpreted in accordance with applicable Data Protection Legislation; and

**Software and Services** shall have the meaning set forth in the Changefirst Master Agreement and appropriate Schedule of Works (SOW).

### DATA PROTECTION

1. The provisions of this Section 1 shall apply to the Client Personal Data we process while providing the Services. Changefirst is the data processor in relation to Client Personal Data. See Sections 7-11 below.
2. The subject-matter of the data processing is providing the Services and the processing will be carried out until we cease to provide any Services to you, the Client. Specifically, Section 9 sets out the nature and purpose of the processing, the types of Client Personal Data we the Changefirst process and the data subjects whose Client Personal Data is processed.
3. When we process Client Personal Data while providing Services to the Client, we the Changefirst will:
  - 3.1. process the Client Personal Data only in accordance with documented instructions from you (as set forth in this Schedule or the Agreement). If applicable law requires us to process the Client Personal Data for any other purpose, the Changefirst will inform you of this requirement first, unless such law(s) prohibit this on important grounds of public interest,
  - 3.2. notify the Client promptly if, in the Changefirst's opinion, an instruction for the processing of Client Personal Data given by you the Client infringes applicable Data Protection Legislation,
  - 3.3. ensure compliance with the obligations pursuant to Chapter 3 of the General Data Protection Regulation,
  - 3.4. assist the Client, considering the nature of the processing, by:
    - 3.4.1. appropriate technical and organisational measures and where possible, in fulfilling the Clients obligations to respond to requests from data subjects exercising their rights,
    - 3.4.2. ensuring compliance with the obligations pursuant to Articles 32 to 36 of the General Data Protection Regulation, considering the information available to us and
    - 3.4.3. making available to you all information reasonably requested by you for the purpose of demonstrating that your obligations relating to the appointment of processors as set out in Article 28 of the General Data Protection Regulation have been met.
    - 3.4.4. implementing and maintaining appropriate technical and organisational measures (See Sections 12-21 – Description of Technical and Organizational Measures – below) to protect the Client Personal Data against unauthorised or unlawful processing and against accidental loss, destruction, damage, theft, alteration, or disclosure. These measures shall be appropriate to the harm which might result from any unauthorised or unlawful processing, accidental loss, destruction, damage, or theft of Client Personal Data and appropriate to the nature of the Client Personal Data which is to be protected. Changefirst may amend the technical and organisational measures, provided that the new measures do not fall short of the level of security provided by the specified measures. Substantial changes must be documented,

## Changefirst Ltd Data Processing Agreement

- 3.4.5. not giving access to or transferring any Client Personal Data to any third party for such third party's independent use (e.g., not directly related to providing the Services) without the Client's prior written consent. Client consents to Changefirst's appointment of the sub-processors listed in Section 11. Changefirst will notify the Client in writing of any changes to the list of approved sub-processors, at which point you will have the opportunity to object by terminating the Agreement. When engaging sub-processors in the processing of Client Personal Data, we are responsible for the conduct and performance of each sub-processor. Changefirst will include in our agreement with any such third-party sub-processor terms which are at least as favourable to you as those contained herein and as are required by applicable Data Protection Legislation,
  - 3.4.6. ensuring that our personnel required to access the Client Personal Data are subject to a binding duty of confidentiality regarding such Client Personal Data,
  - 3.4.7. except as set forth in Section 3.4.4 above or in accordance with documented instructions from the Client (as set forth in this, or the Master, Agreement), ensuring that none of our personnel publish, disclose or divulge any Client Personal Data to any third party,
  - 3.4.8. upon expiration or earlier termination of the Agreement, upon the Client's written request, securely destroying or returning to the Client, such Client Personal Data, and destroy existing copies unless applicable laws require storage of such Client Personal Data; and
  - 3.4.9. at our option, allowing you and your authorised representatives to either (i) access and review up-to-date attestations, reports or extracts thereof from independent bodies (e.g., external auditors, internal audit, data protection auditors) or suitable certifications to ensure compliance with the terms of this Schedule; or (ii) conduct audits or inspections during the term of the Agreement to ensure compliance with the terms of this Schedule in accordance with this Section 1.3.9. Notwithstanding the foregoing, any audit must be conducted during regular business hours, with reasonable advance notice to the Changefirst and subject to reasonable confidentiality procedures. In addition, audits shall be limited to once per year, unless (a) Changefirst has experienced a Security Breach within the prior twelve (12) months; or (b) an audit reveals a material noncompliance.
- 3.5. If the Changefirst becomes aware of and confirm any accidental, unauthorised, or unlawful destruction, loss, alteration, or disclosure of, or access to your Client Personal Data that we process in the course of providing the Services (a 'Security Breach'), the Changefirst shall notify the Client within forty-eight hours.
- 3.6. Through the use of the Services, as further described in the Agreement, Client may elect to grant third parties' visibility to Client data or content (which may include Client Personal Data). Nothing in this Policy prohibits (and, for the avoidance of doubt, Sections 3.4.4 and 3.4.6 above do not apply to) Changefirst making visible your data or content (which may include Client Personal Data) to third parties consistent with this paragraph, as directed by users through the Services.

### MISCELLANEOUS

- 4. Where the Client uses multiple of our Services, Client acknowledges that Changefirst may combine information from Client's use of the Services to deliver integrated services that Client may have purchased (for example to allow search across the services or to combine notifications from multiple services). To allow Changefirst to improve, benchmark and develop our services, Client acknowledges that Changefirst may process information generated by the Client's users subject to appropriate technical and organisational measures for the purposes described in this Schedule.
- 5. In the event of any conflict or inconsistency between the provisions of the Agreement and this Schedule, the provisions of this Schedule shall prevail. For avoidance of doubt and to the extent allowed by applicable law, all liability under this Schedule will be governed by the relevant provisions of the Agreement, including limitations of liability. Save as specifically modified and amended in this Schedule, all the terms, provisions and requirements contained in the Agreement shall remain in full force and effect and govern this Schedule. Except as otherwise expressly provided herein, no supplement, modification, or amendment of this Schedule will be binding, unless executed in writing by a duly authorised representative of each party to this Schedule. If any provision of the Schedule is held illegal or unenforceable in a judicial proceeding, such provision shall be severed and shall be inoperative, and the remainder of this Schedule shall remain operative and binding on the parties.

Changefirst Ltd  
Data Processing Agreement

6. This Schedule shall be governed and construed in accordance with the laws of England (in relation to contractual and non-contractual matters). The Parties irrevocably submit to the exclusive jurisdiction of the English Courts in respect of any matter, claim or dispute arising under, out of or in connection with this Agreement (including as to its validity and in relation to contractual and non-contractual matters) or the legal relationships established by this Agreement.

#### DESCRIPTION OF DATA PROCESSING

7. **Subject-Matter** - Providing, blocking and deleting access to the Service.
8. **Duration** - The term of the agreement as defined in the Services SOW.
9. **Extent, Type and Purpose of the Processing** - the Personal Data transferred will be subject to the following basic processing activities:
- For delivery and provision of the Products & Services,
  - For customer support and technical troubleshooting,
  - For Changefirst' business operations,
  - To improve existing and create new products and services,
  - To market to users and customers,
  - For research and analytics,
  - To comply with law, including law enforcement requests,
  - To prevent fraud and mitigate risk to Changefirst and others.
10. **Data Subjects and Categories of Data** - the types of Personal Data that shall be Processed in accordance with this Agreement will be:
- Direct identifying information (e.g., first and last name, email address, unique ID)
  - Indirect identifying information (e.g., location (country))
  - Device identification data and traffic data (e.g., IP addresses, web logs).
  - Any personal data supplied by users of the Products & Services.

Changefirst does not knowingly and does not want to (and Client/user shall not submit) collect any special categories of data (as defined under Data Protection Legislation).

The category of Data Subjects whose Personal Data will be Processed in accordance with this Agreement will be Employees of client (including client advisors).

11. **Approved Sub-Processors & Sub Contractors** - the Client hereby consents to the Changefirst appointing and using the following sub-processors and subcontractors: [info.changefirst.com/sub-processors](https://info.changefirst.com/sub-processors).

#### DESCRIPTION OF TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

12. The following information describes the technical and organizational security measures and controls implemented by Changefirst to protect Personal Data and ensure the ongoing confidentiality, integrity and availability of the Changefirst Service – Roadmap Pro.
13. Changefirst is certified to the standard of ISO 27001 and take information security seriously. Relevant information security policies are listed alongside each measure taken below in respect of the management system in place. Changefirst uses processes and procedures in respect of the security management and handling of Personal Data.
14. As of the Effective Date of the Agreement, Changefirst, when Processing Client Personal Data in connection with the Service, shall implement and maintain the following technical and organizational security measures for the Processing of such Personal Data.

Changefirst Ltd  
Data Processing Agreement

15. **Access control to premises and facilities** - technical and organizational measures to control access to premises and facilities, particularly to check authorization:
- Changefirst Services production systems located in ISO 27001 certified, professional, third-party data center facilities with a defined and protected physical perimeter, strong physical controls including access control mechanisms, surveillance and 24x7x365 guards. Only authorized representatives have access to the data center premises.
  - Changefirst business premises are secured with access control mechanisms. Only authorized personnel have privileged access to internal systems.
  - Changefirst have access control and privileged access control policies.
16. **Access control to systems** - technical (ID/password security) and organizational (user master data) measures for user identification and authentication:
- Changefirst use appropriate measures to prevent Personal Data from being used without authorization. These controls shall vary based on the nature of the Processing undertaken and may include, among other controls, multiple authentication methods, documented authorization processes, documented change management processes and/or logging of access.
  - Changefirst have access control, password management and privileged access control policies.
17. **Access control to data** - requirements-driven definition of the authorization scheme and access rights, and monitoring and logging of accesses:
- Changefirst use appropriate measures to provide that Personal Data is accessible and manageable only by properly authorized staff, direct database query access if restricted and application access rights are established and enforced to ensure that persons entitled to use a data processing system only have access to the Personal Data to which they have privilege of access; and, that Personal Data cannot be read, copied, modified or removed without authorization in the course of Processing.
  - When Personal Data is copied electronically by Changefirst outside of its managed systems, appropriate physical security is maintained, and data encrypted when necessary.
  - Changefirst have access control and privileged access control policies and an information classification and handling procedure.
18. **Disclosure control** - measures to transport, transmit and communicate or store data on data media (manual or electronic) and for subsequent checking:
- Changefirst use appropriate measures to ensure that it is possible to check and establish to which entities the transfer of Personal Data by means of data transmission facilities is envisaged so Service Data cannot be read, copied, modified or removed without authorization during electronic transmission or transport.
  - Changefirst have data encryption and data transfer policies.
19. **Input control** - measures for subsequent checking whether data have been entered, changed or removed (deleted), and by whom:
- Changefirst use appropriate measures to check and establish whether and by whom Service Data has been entered into data processing systems, modified or removed.
  - Changefirst ensure that (i) the Personal Data source is under the control of Data Controller and (ii) Personal Data integrated into the Service is managed by secured transmission from Data Controller.
  - Changefirst have event logging (including user and admin events) set up in our user management systems.
  - Events are stored in the production database for a limited time for review when required.
20. **Job control** - measures (technical/organizational) to segregate the responsibilities between the Data Controller and the Data Processor:

## Changefirst Ltd Data Processing Agreement

- Changefirst acts (dependent on the situation) as data controller and/or data processor with respect to Personal Data and stores and processes Personal Data to provide Change Management Services under the instructions of a Customer.
- Changefirst does not access Personal Data, except to provide services to the Customer which Changefirst is obligated to perform in support of the Customer experience including for general operation and monitoring of our Change Management Services, troubleshooting and maintenance purposes, for security reasons, as required by law, or on request by a Customer.
- Changefirst engage with sub-processors to help provide our Services. This list is available to view at: <https://info.changefirst.com/sub-processors>.
- Changefirst have a supplier security policy.

21. **Availability control** - measures to assure data security (physical/logical):

- Changefirst have a business continuity management policy and disaster recovery plans.

22. **Segregation control** - measures to provide for separate Processing (storage, amendment, deletion, transmission) of data for different purposes:

- In each step of the processing, Personal Data is associated in logically segregated Customer environments.
- Data Controllers have access only to their own Personal Data.
- Audit rights given to Data Controllers always exclude the right or ability to look at the data of other Changefirst Customers.