Data Processing Agreement

Insofar as Fourth Enterprises, LLC, Fourth Ltd. and any of their affiliates ("**Data Processor**") will be processing personal data on behalf of its subscribers and customers ("**Data Controller**") in the course of providing its products and services (**"Services"**), the terms of this Data Processing Agreement ("**Agreement**") shall apply. References to "**Data Protection Laws**" shall mean any law applicable to Data Processor's processing or use of personal data, including (to the extent applicable), Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and any corresponding or equivalent national data protection laws made under, pursuant to such Regulation, including enacting or amending legislation ("**GDPR**"), and The California Consumer Privacy Act of 2018, AB375, Title 1.81.5, including any implementing law, as amended ("**CCPA**").

This Agreement does not cover any personal information or data collected by Data Processor for other purposes, such as information collected directly from individuals who use Data Processor's websites or mobile applications for their own purposes. The policy followed by Data Processor in connection with such direct user information is available at https://www.fourth.com/privacy-policy/.

1. **Collection.** Data Processor collects personal information through the input fields filled in by the Data Controller's employees and other users of the Services or where data is otherwise transferred to the Data Processor. Data Processor may also use cookies, log files, web beacons, device identifiers, advertising identifiers, and similar tracking technologies, including those from third-party service providers like Google Analytics and other cloud-based tools, to automatically collect preferences, performance data, and information about access and use of the Services. Data Processor provides more information about how it utilizes cookies at https://www.fourth.com/en-gb/legal/cookie-policy-solutions-and-applications/. Data Controller provides the Data Processor with the following personal data in the course of using the Services:

    - The subject matter of processing the personal data by the Data processor is the performance of the Services.
    - The duration of processing will be the period that the Data Processor provides the Services to the Data Controller.
    - The nature and purpose of processing is for the Data Processor to process the personal data in order to perform the Services.
    - The relevant data subject will be any individual about whom data is transferred to the Data Processor as part of the Services.

Type and categories of personal data (if shared by the Data Controller as part of the Services)	Do we collect?	Do we disclose for a business purpose(s)
Name, Contact Info and other Identifiers: identifiers such as a name, alias, address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number or state identification card number, driver's license number, passport number, or other similar identifiers.	*Yes*	*Yes*

Customer Records: paper and electronic customer records containing personal data, such as name, signature, physical characteristics or description, address, telephone number, education, current employment, employment history and associated documentation, social security number, passport number, driver's license or state identification card number, insurance policy number, bank account number, credit card number, debit card number, or any other financial or payment information, medical information, or health insurance information.	*Yes*	*Yes*
Protected Classifications/Characteristics: characteristics of protected classifications under Data Protection Laws such as race, color, sex, age, religion/belief, nationality, ethnic origin, pregnancy/maternity, gender reassignment, marriage and civil partnership, disability, citizenship status, and genetic information.	*Yes*	*Yes*
Purchase History and Tendencies: commercial information including records of personal property, products or services purchased, obtained, or considered, or other purchasing or use histories or tendencies.	*No*	*No*
Biometric Information: physiological, biological, or behavioral characteristics that can be used alone or in combination with each other to establish individual identity, including DNA, imagery of the iris, retina, fingerprint, faceprint, hand, palm, vein patterns, and voice recordings, keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.	*Yes*	*Yes*
Special categories of data (only where provided by the Data Controller): data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation	*Yes*	*Yes*
Usage Data: internet or other electronic network activity information, including, but not limited to, browsing history, clickstream data, search history, and information regarding a resident's interaction with the SaaS platform, website, application, or advertisement.	*Yes*	*Yes*
Geolocation Data: precise geographic location information about a particular individual or device.	*No*	*No*
Audio, Video and other Electronic Data: audio, electronic, visual, thermal, olfactory, or similar information.	*Yes*	*Yes*
Employment History: professional or employment-related information.	*Yes*	*Yes*
Education Information: information about education history or background that is not publicly available personally identifiable information as defined in the federal Family Educational Rights and Privacy Act (20 U.S.C. section 1232g, 34 C.F.R. Part 99).	*Yes*	*Yes*

Profiles and Inferences: inferences drawn from any of the information identified above to create a profile reflecting a resident's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.	*No*	*No*

2. Processing.

a) Data Processor will only process, store, and use the personal data it receives from the Data Controller as necessary to provide the Services, perform to Data Controller's prior written instructions (including with regard to international transfers), or as otherwise agreed by the parties. The Data Processor shall notify Data Controller immediately if, in its opinion, an instruction infringes Data Protection Law. The Data Processor shall never retain, use, disclose, sell, or process the personal data other than as specified in this Agreement, the Data Controller's documented instructions, or as otherwise permitted by law. The Data Controller agrees that Data Processor may store and delete personal data in accordance with its Data Retention Policy, available at https://www.fourth.com/en-gb/wp-content/uploads/sites/2/2019/10/Data-Retention-Policy-March-2018-FINAL.pdf, as amended by Data Processor from time to time. Upon termination of the provision of Services by the Data Processor, the Data Processor shall, at the choice of the Data Controller, delete (in accordance with its policies from time to time) or return to the Data Controller the personal data (unless storage is required by law).

b) The Data Controller represents and warrants that it has all necessary rights to provide the personal data to the Data Processor for the processing to be performed in connection with the Services. To the extent required by Data Protection Laws, the Data Controller is responsible for providing all necessary privacy notices to data subjects and ensuring that it has the appropriate legal basis under Data Protection Laws for the processing required under the Agreement, including the transfer of Personal Data to Data Processor. Should the Data Controller cease to have such a legal basis to process the personal data (or to transfer it to the Data Processor) it will inform the Data Processor of such fact, and the Data Processor is responsible for implementing Data Controller's instruction with respect to the processing of such personal data. Data Controller will keep the personal data accurate and fully up to date at all times during the continuance of the Services.

3. Confidentiality.

The Data Processor shall treat all personal data confidentially and will take steps to protect personal data that are substantially similar to those it takes to protect its own personal data (but not less than reasonable care) to prevent its unauthorized disclosure. Except as otherwise expressly set forth in this Agreement, the Data Processor shall not disclose or process the personal data without the prior written consent of Data Controller, except for the purpose of exercising its rights or performing its obligations under this Agreement. The Data Processor shall inform all its employees, agents and approved sub-processors engaged in processing the personal data of the confidential nature of the personal data. The Data Processor shall cause all such persons or parties to sign agreements with confidentiality obligations no less restrictive in the use and protection of the personal data than those Data Processor has to Data Controller.

4. Security Measures.

a) Considering the state of the art, the costs of implementation and the nature, scope, context, and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Data Processor shall implement appropriate technical and organizational security measures commensurate with the risk involved in the processing. The Data

Processor shall maintain and follow written security policies that are fully implemented and applicable to the processing of personal data. At a minimum, such policies will include assigning internal responsibility for information security management, devoting adequate personnel resources to information security, carrying out verification checks on permanent staff who will have access to the personal data (to the extent permitted by local law), conducting appropriate background checks (to the extent permitted by local law), requiring employees, vendors, and others with access to personal data to enter into written confidentiality agreements, and conducting training to make employees and others with access to the personal data aware of information security risks presented by the processing.

b) At the request of the Data Controller, the Data Processor shall demonstrate to the Data Controller the measures it has taken pursuant to this Article 4 and shall allow the Data Controller to audit and test such measures, to the extent it does not require providing access to the data of others and following signature of a confidentiality agreement if requested by the Data Processor. Subject to such restriction, the Data Processor shall cooperate with such audits carried out by the Data Controller, shall grant the Data Controller´s approved auditors reasonable access to the Data Controller's personal data to demonstrate compliance with this Agreement (subject to reasonable costs agreed in advance by the parties and limited to one request in a 12 month period), and shall provide such auditors with access to any information relating to the processing of such personal data as may be reasonably required by the Data Controller to ascertain the Data Processor´s compliance with this Agreement.

c) In so far as it is able to, the Data Processor shall assist the Data Controller in ensuring compliance with its obligations with regards to data security, breach notification, privacy impact assessments and consulting with the supervisory authority.

d) Where Data Processor offers a secure method of processing or transmitting personal data and the Data Controller chooses a less secure (or non-secure) method of processing or transmitting personal data, then the Data Processor shall not be liable for any breach of this Agreement or applicable Data Protection Law or liability that occurs or arises from such less secure method of processing.

5. Data Transfers.

This clause only applies to Data Controllers which transfer personal data from the European Economic Area or the United Kingdom to a third country (within the meaning of Regulation (EU) 2016/679), except where there is a European Commission adequacy decision under Article 45 of Regulation (EU) 2016/679 in force which covers such transfer. The parties agree that such personal data transfer is subject to the model contractual clauses annexed to Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (the "Clauses"), which are hereby incorporated into this Agreement. In such cases, Data Controller is the 'data exporter' and Data Processor is the 'data importer' as defined in the Clauses.

6. Security Breach.

The Data Processor will notify the Data Controller without undue delay upon discovery of any personal data breach (as defined by Data Protection Laws). Data Processor will not communicate with any third party regarding any security breach except as specified by Data Controller or by applicable law.

7. Subprocessors.

The Data Processor may subcontract any of its Services-related activities or allow any personal data to be processed by a third party, provided that such subprocessors are bound by the same data protection obligations imposed on the Data Processor under this Agreement. Data Processor shall be responsible for the acts and omissions of its subprocessors in their capacity as such. A current list of subprocessors of the Services is listed at https://www.fourth.com/legal/subprocessors/, which may be updated from time to time. If Data Controller reasonably objects to the addition of any new subprocessor within 10 days of the Data Processor updating its list of subprocessors and it is not possible for the Data Processor to provide the Services without using that subprocessor, it may terminate the applicable Services which rely on that subprocessor as provided in the contract between the parties. In the provision of the Services, if personal data will be transferred from within the EEA or the United Kingdom to a subprocessor in a third country (within the meaning of Regulation (EU) 2016/679), it shall be transferred in accordance with the requirements of the Clauses.

8. Data Subject Rights.

The Data Processor shall assist the Data Controller by appropriate technical and organizational measures, insofar as it is possible, for the fulfilment of the Data Controller's obligation to respond to requests for exercising the data subject's rights under the Data Protection Laws, subject to such reasonable costs as agreed in advance between the parties. With respect to the data processed under this Agreement, an individual who seeks access to or a copy of their personal data, or who seeks to correct, amend, restrict, object or delete inaccurate personal data on the Services, should direct their query to the Data Controller. If the Data Controller requests the Data Processor to remove or provide a copy of the personal data to comply with Data Protection Laws, to the extent that such data is not already available to the Data Processor through their use of the Services, Data Processor will respond to their request within the time period prescribed by law, or if no time period is prescribed, within 30 days, but only in circumstances where Data Controller is not able to access, remove or copy the personal data itself.

9. Comments or Questions.

Any comments or questions relating to this policy can be addressed to security@fourth.com.