|  |  |
| --- | --- |
| C:\Users\DTollen\My ShareSync\Law Practice\Tech Contracts Academy\Admin\Identity\Logo\TCA_TM Logo_FINAL\PNG\Tech-Contracts-Academy-Logo_TM_Color_FINAL.png<https://TechContracts.com/> | **THE TECH CONTRACTS HANDBOOK****Cloud Computing Agreements, Software Licenses, and Other IT Contracts for Lawyers and Businesspeople**Third Edition**by David W. Tollen**(ABA Publishing - Intellectual Property Law Section of the American Bar Association; 2021) |

***Form Contract Attachment***

**Customer’s Data Protection Attachment for all Data**

***Data Management & Security Attachment for Cloud Services Deals; Terms re All Data; Additional Attachments for Specific Laws (GDPR, CCPA, HIPAA, etc.) NOT Included; Customer-Friendly; Corresponds to Tech Contracts Handbook Chapter II.J (excluding Subchapter II.J.8)***

*You may use the form contract below subject to the “Terms of Use” posted at* [*https://techcontracts.com/terms-of-use-and-privacy-policy/*](https://techcontracts.com/terms-of-use-and-privacy-policy/)*. In addition to the Terms of Use, PLEASE READ THE FOLLOWING DISCLAIMER BEFORE USING THE FORM CONTRACT:*

***NEITHER TECH CONTRACTS ACADEMY®, LLC NOR THE AUTHOR OR PUBLISHER, OR ANYONE AFFILIATED WITH THEM, REPRESENTS THAT THE FORM CONTRACT BELOW WILL MEET YOUR SPECIFIC GOALS, PROTECT YOUR SPECIFIC INTERESTS, OR WITHSTAND CHALLENGES TO ITS LEGAL OR FACTUAL SUFFICIENCY. The form contract below is general in nature and may not be sufficient for a specific contractual, technological, or legal problem or dispute. THE FORM IS NOT PROVIDED WITH ANY GUARANTY, WARRANTY, OR REPRESENTATION AS TO QUALITY OR SUITABILITY FOR ANY PARTICULAR PURPOSE. Publication of the form does not constitute the practice of law and is not legal counsel or advice. Neither Tech Contracts Academy®, LLC or the author or the publisher of this website or* The Tech Contracts Handbook*, or anyone affiliated with them, is rendering a legal or other professional service. The form should not be relied upon as a substitute for consultation with an attorney.***

*Note that this document uses Microsoft Word multi-level bullets/numbering for section numbers and cross-referencing features for section references.*

*Please delete all text above the following dotted line, as well as the line itself and the page-break following it, before using this form.*

------------------------------------

**DATA PROTECTION ATTACHMENT**

This Data Protection Attachment (this “Attachment”) is attached to and incorporated into the \_\_\_\_\_\_\_\_ (the “Agreement”) between \_\_\_\_\_ and \_\_\_\_\_. Terms defined in the Agreement have the same meanings in this Attachment.

1. **Data Ownership and License.** Provider recognizes and agrees that Customer possesses and retains all right, title, and interest in and to Customer Data, and Provider’s use and possession thereof is solely on Customer’s behalf. Provider further recognizes and agrees that: (1) Customer Data is valuable property of Customer; (2) Customer Data includes Customer’s trade secrets; (3) Customer Data is an original compilation pursuant to the copyright law of the United States and other jurisdictions; and (4) Customer has dedicated substantial resources to collecting, managing, and compiling Customer Data. Customer hereby grants Provider a limited license to reproduce and otherwise manage Customer Data during the Term solely as specifically authorized below in this Attachment.
2. **Excluded Data.** Customer warrants that (1) it has not and will not transmit Excluded Data (as defined below), or permit transmission of Excluded Data, to Provider or its computers or other media and, (2) to the best of its knowledge, Customer Data does not and will not include Excluded Data. Customer shall inform Provider of any Excluded Data within Customer Data promptly after discovery (without limiting Provider’s rights or remedies). Customer recognizes and agrees that: (a) the provisions below of this Attachment do not apply to Excluded Data; (b) Provider has no liability for any failure to provide protections in the Excluded Data Laws (as defined below) or otherwise to protect Excluded Data; and (c) Provider’s systems are not intended for management or protection of Excluded Data and may not provide adequate or legally required security for Excluded Data. Provider is not responsible or liable for any Data Incident (as defined \_\_) or other loss to the extent that it involves Excluded Data. (“Excluded Data” means \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. “Excluded Data Laws” means any law or regulation governing Excluded Data, including without limitation any law or regulation protecting privacy or security rights of Excluded Data subjects, as well as the following statutes and regulations: \_\_\_\_\_\_\_\_\_\_\_\_.)
3. **Use and Disclosure.** Provider may access and use Customer Data solely as necessary to provide the System to Customer, and unless it receives Customer’s prior written consent, Provider: (1) shall not access or use Customer Data for any purpose other than to provide the System; and (2) shall not give any third party access to Customer Data, except subcontractors subject to Section M (Employees and Subcontractors) of this Attachment. Notwithstanding the provisions above of this Section C, Provider may disclose Customer Data as required by applicable law or by proper legal or governmental authority. Provider shall give Customer prompt notice of any such legal or governmental demand and reasonably cooperate with Customer in any effort to seek a protective order or otherwise to contest such required disclosure, at Customer’s expense. For the avoidance of doubt, no revision of Provider’s privacy policy will alter Customer’s rights and remedies in this Attachment.
4. **Aggregate/Anonymized Data.** Notwithstanding Section C (Use and Disclosure) of this Attachment, Customer hereby authorizes Provider: (1) to Anonymize (as defined below) Customer Data and to combine it with data from other customers into a new aggregate dataset; and (2) to use such Anonymized Customer Data as a component of such new aggregate dataset for any legal business purpose, including without limitation for distribution to third parties. Without limiting the generality of the requirements for Anonymized data below, Provider shall: (a) implement technical safeguards that prohibit reversal of Anonymization of Customer Data; (b) implement business processes that specifically prohibit such reversal or recreation; (c) make no attempt to achieve such reversal; and (d) implement reasonable business processes to prevent inadvertent release of Anonymized Customer Data. (“Anonymize” refers to removal of Personal Information and any information reasonably likely to identify a company or other business entity; provided such revised data does not include and is not subject to any key, code, or other mechanism that could be used to restore such information.)
5. **Injunction and Enforcement.** Provider agrees that: (1) no adequate remedy exists at law if it fails to perform or breaches any of its obligations in this Attachment; (2) it would be difficult to determine the damages resulting from its breach of this Attachment, and such breach would cause irreparable harm to Customer; and (3) a grant of injunctive relieve provides the best remedy for any such breach, without any requirement that Customer prove actual damage or post a bond or other security. Provider waives any opposition to such injunctive relief or any right to such proof, bond, or other security. Provider’s obligations in this Attachment (without limitation) apply likewise to Provider’s successors, including without limitation to any trustee in bankruptcy. (This Section E does not limit either party’s right to injunctive relief from breaches not listed.)
6. **Privacy and Security Law Compliance.** Provider shall comply with all applicable laws and regulations governing Provider’s access to, use of, and handling of Customer Data; provided the foregoing does not require that Provider comply with or be aware of any Excluded Data Law.
7. **Statutory Special Terms.**
	1. The parties recognize and agree that Addendum \_\_ attached to this Attachment: (a) governs the following Customer Data: \_\_\_\_\_\_\_\_\_\_ [list the data governed by the privacy/security law in question – or create multiple addenda if multiple such laws apply]; and (b) applies only to such Customer Data and not to any of the parties’ other rights or duties pursuant to this Attachment or this Agreement.
	2. Provider shall \_\_\_\_\_\_\_\_\_\_ [insert additional statutory special terms, if any].
	3. If Provider receives a consumer “right to know,” deletion, “right to be forgotten,” or similar request related to Personal Information within Customer Data (collectively, “Consumer Requests”), Provider shall not reply without Customer’s written authorization and shall, at its own expense, comply with Customer’s reasonable written instructions for Consumer Requests (if any), subject to the requirements of applicable law. Notwithstanding the preceding sentence, nothing in this Agreement precludes Provider from asserting defenses or rights it may have under applicable law related to Consumer Requests.
8. **Approved Region and Data Centers.** Provider shall not transfer Customer Data (or allow its subcontractors to transfer Customer Data): outside \_\_\_\_\_\_\_\_\_ (the “Approved Territory”) unless it receives Customer’s prior written consent. Further, except as provided in Section \_\_ (Business Continuity) of this Agreement’s main body, provider shall not transfer Customer Data to any location other than the data centers listed \_\_\_\_\_\_\_\_, unless such replacement data center complies with the requirements of this Attachment and unless Provider gives Customer \_\_\_ business days’ prior written notice.
9. **Customer Access and e-Discovery.** Customer may access and copy any Customer Data in Provider’s possession at any time. Provider shall reasonably facilitate such access and copying promptly after Customer’s request, provided Provider may charge its reasonable then-standard fees for any such access and copying or for any related deconversion of data.
10. **Deletion.** Except as required by applicable law or authorized pursuant to a data deletion policy accepted in writing by each party, Provider shall not erase Customer Data or any copy thereof without Customer’s prior written consent. Further, Provider shall: (1) halt Customer Data deletion promptly if Customer informs Provider that any Customer Data is subject to “e-discovery” or otherwise relevant to potential litigation; (2) at such times as Customer may request (including without limitation as a result of Consumer Requests made mandatory by applicable law), promptly erase all Customer Data from all systems under Provider’s control and direct and ensure erasure by any and all of its subcontractors that have access to Customer Data; and (3) within \_\_ days of termination (including without limitation expiration) of this Agreement, erase all Customer Data in Provider’s possession or control, including without limitation in the possession or control of its subcontractors, subject to Provider’s rights above (if any) in Section D (Aggregate/Anonymized Data) of this Attachment. In erasing Customer Data as required by this Agreement, Provider shall leave no data readable, decipherable, or recoverable on its computers or other media or those of its subcontractors, using the best erasure methods commercially feasible. Promptly after any erasure of Customer Data or any part of it, Provider shall certify such erasure to Customer in writing.
11. **General Security.** Without limiting the generality of its obligations elsewhere in this Attachment, Provider shall exercise commercially reasonably efforts to prevent unauthorized exposure or disclosure of Customer Data.
12. **InfoSec Program.** Provider shall maintain, implement, and comply with a written data and information security program (the “InfoSec Program”) that requires administrative, technical, and physical safeguards appropriate: (1) to protect the security and confidentiality of Customer Data; (2) to protect against anticipated threats or hazards to the security or integrity of Customer Data; and (3) to protect against unauthorized access to or use of Customer Data. Provider shall likewise ensure that the InfoSec Program includes and requires compliance with the following (without limitation): (4) guidelines on the proper disposal of Customer Data after it is no longer needed to carry out the purposes of this Agreement, consistent with the requirements Section J (Deletion) of this Attachment; (5) access controls on electronic systems used to maintain, access, or transmit Customer Data; (6) access restrictions at physical locations containing Customer Data; (7) encryption of electronic Customer Data consistent with then-current nationally-recognized encryption standards; (8) least privilege principles for access to Customer Data, supplemented either by dual control procedures or segregation of duties; (9) regular testing and monitoring of electronic systems accessing or storing Customer Data; and (10) procedures to detect actual and attempted attacks on or intrusions into the systems containing or accessing Customer Data. Provider shall review the InfoSec Program and all other Customer Data security precautions regularly, but no less than annually, and update them to comply with applicable laws, regulations, technology changes, and best practices.
13. **Employees and Subcontractors.** Provider shall not permit any of its employees, subcontractors, or subcontractor employees to access Customer Data except to the extent that such individual or company needs access to facilitate the System and is subject to a reasonable written agreement with Provider, or in case of employees, a reasonable written employment policy, protecting such data, with terms consistent with those of this Attachment. Further, Provider shall not allow any individual to access Customer Data except to the extent that he or she has received a clean report with regard to each of the following: (1) verifications of education and work history; (2) a 7-year all residence criminal offender record information check; and (3) a 7-year federal criminal offender record information check. (A clean report refers to a report with no discrepancies in education or work history and no criminal investigations or convictions related to felonies or to crimes involving identity theft or other misuse of sensitive information.) However, Subsections M(2) and M(3) do not apply to the extent that applicable law forbids the required record information check, provided Provider notifies Customer of such restriction. Without limiting the generality of Provider’s obligations related to subcontractors and their employees, Provider shall exercise reasonable efforts to ensure that each subcontractor complies with the terms of this Agreement related to Customer Data. As between Provider and Customer, Provider shall pay any fees or costs related to each subcontractor’s compliance with such terms.
14. **Audits.** Provider shall retain a certified public accounting firm to perform an annual audit of the System’s data protection features and to provide a SOC 2 Type II report, pursuant to the then-current standards of the American Institute of Certified Public Accountants (the “AICPA”). If the AICPA revises its relevant reporting standards, Provider shall retain such accounting firm to provide the report that then most resembles a SOC 2 Type II report. In addition, Provider shall annually conduct its own internal security audit and address security gaps. Provider shall give Customer a copy of the most current report from each audit listed above in this Section N within \_\_ business days of the Effective Date and thereafter annually within \_\_ business days of completion of thereof.
15. **Customer Testing.** If requested by Customer, Provider shall, on a quarterly basis: (1) permit security reviews by Customer on systems storing or processing Customer Data and on Provider policies and procedures relating to the foregoing, including without limitation the InfoSec Program; and (2) permit testing of all security processes and procedures during the Term, including without limitation penetration tests. Notwithstanding the foregoing, Provider is not required to permit any review or inspection that may compromise the security of Provider’s other customers’ data.
16. **Audit and Test Results.** Any report or other result generated through the tests or audits required by Section N (*Audits*) or O (*Customer Testing*) of this Attachment will be Provider’s Confidential Information pursuant to Section \_\_ (Confidential Information) of this Agreement’s main body. If any audit or test referenced above uncovers deficiencies or identifies suggested changes in Provider’s provision of the System, Provider shall exercise reasonable efforts promptly to address such deficiencies and changes, including without limitation by revising the InfoSec Program.
17. **Data Incidents.** Provider shall implement and maintain a program for managing unauthorized disclosure of, access to, or use of Customer Data (“Data Incidents”). In case of a Data Incident, or if Provider suspects a Data Incident, Provider shall: (1) promptly, and in any case within 48 hours, notify Customer by telephone, in person, or by other real-time, in-person communication; (2) cooperate with Customer and law enforcement agencies, where applicable, to investigate and resolve the Data Incident, including without limitation by providing reasonable assistance to Customer in notifying injured third parties; and (3) otherwise comply with applicable laws governing data breach notification and response. In addition, if the Data Incident results from Provider’s breach of this Agreement or negligent or unauthorized act or omission, including without limitation those of its subcontractors or other agents, Provider shall (a) compensate Customer for any reasonable expense related to notification of consumers and (b) provide 1 year of credit monitoring service to any affected individual. Provider shall give Customer prompt access to such records related to a Data Incident as Customer may reasonably request, and such records will be Provider’s Confidential Information pursuant to Section \_\_ (Confidential Information) of this Agreement’s main body; provided Provider is not required to give Customer access to records that might compromising the security of Provider’s other customers. This Section Q does not limit Customer’s other rights or remedies, if any, resulting from a Data Incident.