Template Vendor Privacy & Security Terms
25 September 2016

A. Background

Many US and international laws require companies to enter into written contracts with data processors to ensure the security and confidentiality of personal information. For example, California law requires businesses that disclose personal information to vendors to contractually bind the vendors to implement and maintain reasonable and appropriate security procedures to protect the information.[1] Similar laws exist today in many US states and international jurisdictions.

In Europe, the General Data Protection Regulation (GDPR) imposes specific obligation on companies (controllers) with regard to their vendor relationships. The GDPR requires companies to conduct appropriate due diligence on processes and to have contracts containing specific, defined provisions. In particular, Article 28 of the GDPR provides (in relevant part):

Article 28: **Processor**

1. Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.
2. The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.
3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:

   (a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

   (b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

   (c) takes all measures required pursuant to Article 32 [security];

[1] California Civil Code Section 1798.81.5

(d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;

(e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;

(f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 [security, breach notification, DPIAs, and prior consultation] taking into account the nature of processing and the information available to the processor;

(g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data; [and]

(h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.

4. Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

5. Adherence of a processor to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of this Article.

6. Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 3 and 4 of this Article may be based, in whole or in part, on standard contractual clauses referred to in paragraphs 7 and 8 of this Article, including when they are part of a certification granted to the controller or processor pursuant to Articles 42 and 43.

7. The Commission may lay down standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the examination procedure referred to in Article 93(2).

8. A supervisory authority may adopt standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the consistency mechanism referred to in Article 63.
9. The contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including in electronic form.
10. Without prejudice to Articles 82, 83 and 84, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.

B. Motivation for the Template

This template Vendor Privacy and Security Terms is designed to allow companies and their processors address legal compliance obligations in a fair and balanced manner. These terms appreciate that all companies need flexibility in their contracting processes, but they also recognize that consistency in vendor agreements offers three important benefits. Most importantly, uniform terms help ensure that companies and vendors have shared expectations around privacy and security. Second, uniform terms make administration of contracts simple and cost effective for both parties. Additionally, consistent terms help ensure that all clients and vendors are treated fairly.

No form agreement can address all of the needs that companies may have in a vendor relationship. If the vendor will be processing highly sensitive personal information, for example, additional security provisions will be needed. These additional requirements should be identified during the vendor assessment process. Similarly, no form agreement can address every concern raised by a vendor.

These template terms are annotated to help companies and vendors understand the rationale for some of the provisions included. For example, the annotations indicated which provisions are needed to address the GDPR requirements above. Additionally, the annotation includes optional text changes that can be made to address common concerns. To use this document, thee [green text in brackets] represents a comment to the reader, while blue text represents additional, optional or alternative terms.

Please note that these terms do not include provisions related to indemnification, limitations of liability, and similar clauses that are meant to allocate risks in the relationship. These provisions should be addressed in the underlying services agreement or negotiated separately between the parties.

Companies using this template should identify specific individuals within their legal departments, procurement and/or the privacy office who can provide subject matter expertise on privacy and security requirements applicable to the business, given the specific situations.

Template Standard Vendor Privacy & Security Terms [2]
[Exhibit X to the Services Agreement]

Vendor agrees that it shall comply with the following provisions with respect to all "Personal Information" collected, used, transmitted or maintained for [Acme Industries, Inc.] [and its affiliates] ([collectively,] "Acme"). This Addendum stipulates privacy, confidentiality, and security requirements and demonstrates compliance with applicable privacy, security and data protection laws.

1. Definitions. [Align with definitions in company privacy and security policies and training materials.]

(a) "EEA Personal Data" means personal data (as defined in GDPR) pertaining to residents of the European Economic Area (EEA) and Switzerland.

(b) "GDPR" means Regulation (EU) 2016/679, the General Data Protection Regulation.

(c) "Internal Control Report" means a Type II Service Organizational Control (SOC) report (based on the SSAE 16 or ISAE 3402 model) or any successor report thereto.

(d) "Personal Information" means any and all data (regardless of format) that (i) identifies or can be used to identify, contact or locate a natural person, or (ii) pertains in any way to an identified natural person. Personal Information includes obvious identifiers (such as names, addresses, email addresses, phone numbers and identification numbers) as well as biometric data, "personal data" (as defined in the GDPR) and any and all information about an individual's computer or mobile device or technology usage, including (for example) IP address, MAC address, unique device identifiers, unique identifies set in cookies, and any information passively captured about a person's online activities, browsing, application or hotspot usage or device location. [Adjust this list to reflect specific data elements that the vendor may be processing.]

(e) "Privacy Laws" means all applicable U.S. and international laws that regulate the Processing of Personal Information. In particular, "Privacy Laws" includes [list applicable laws], the GDPR and other applicable laws that specify privacy, security or security breach notification obligations that affect the Personal Information or the provision of the services by Vendor.

(f) "Processing" means any operation or set of operations which is performed upon Personal Information, whether or not by automatic means, such as collection, compilation, use, disclosure, duplication, organization, storage, alteration, Transfer, transmission, combination, redaction, erasure, or destruction.

(g) "Security Breach" means a "personal data breach" (as defined in the GDPR), a "breach of the security of a system" or similar term (as defined in any other applicable Privacy Law or any other event that compromises the security, confidentiality or integrity of Personal Information.

[2] **This template is provided for reference purposes only. Many countries have enacted laws with specific requirements for vendor contracts. This template is NOT designed to address all possible applicable requirements of these laws. Prior to entering into any vendor contract, please consult your own legal counsel to determine the specific requirements that will be applicable, given your particular situation.**

(h) "Sensitive Personal Information" is a subset of Personal Information, which due to its nature has been classified by law or by Acme policy as deserving additional privacy and security protections. Sensitive Personal Information consists of: (i) all government-issued identification numbers, (ii) all financial account numbers (including payment card information and health insurance numbers), (iii) individual medical records, genetic and biometric information, (iv) all data obtained from a U.S. consumer reporting agency (such as employee background investigation reports, credit reports, and credit scores), (v) user account credentials, such as usernames, passwords, security questions/answers and other password recovery data, (v) data elements that constitute Special Categories of Data under the GDPR, namely [EEA Personal 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, [and (vi) list any other Personal Information designated by Acme as Sensitive Personal Information].

(i) "Services" means any and all services that Acme requests the Vendor to perform under [the Agreement] or any other contract or agreement that involves Processing of Personal Information.

(j) "Subprocessor" means any third party (including an affiliate of Vendor) that provides any services to Vendor and that may have access (including inadvertent access) to any [unencrypted] Acme Personal Information.

(k) "Transfer" means to disclose or otherwise make the Personal Information available to a third party (including to any affiliate or Subprocessor of Vendor), either by physical movement of the Personal Data to such third party or by enabling access to the Personal Data by other means.

2. <u>General Obligations</u>.

(a) Vendor shall only Process or Transfer Personal Information as authorized by Acme and as necessary to perform the Services. [GDPR 28(3)(a)]

(b) Vendor shall promptly inform Acme in writing: (i) if it cannot comply with any material term of its agreement with Acme regarding the Services (if this occurs, Vendor shall use reasonable efforts to remedy the non-compliance, and Acme shall be entitled to terminate Vendor's further Processing of Personal Information); (ii) of any request for access to any Personal Information received from an individual who is (or claims to be) the subject of the data; (iii) of any request for access to any Personal Information received by Vendor from any government official (including any data protection agency or law enforcement agency) unless it is explicitly prohibited by law from notifying Acme of the request; (iv) of any other requests with respect to Personal Information received from Acme's employees or other third parties, other than those set forth in the agreement. Vendor understands that it is not authorized to respond to these requests, unless explicitly authorized by Acme or the response is legally required under a subpoena or similar legal document issued by a government agency that compels disclosure by Vendor.

(c) Each party must [use reasonable efforts to] stay informed of the legal and regulatory requirements for its Processing of Personal Information. Vendor's Processing shall comply with all Privacy Laws that are applicable to the Processing, as well as Vendor's own privacy notices.

[Vendor certifies that it is now and shall remain in compliance with all applicable requirements, including (without limitation) Massachusetts 201 CMR 17.00: Standards for The Protection of Personal Information of Residents of the Commonwealth and similar state statutes.]

(d) Vendor has provided Acme with responses to Acme's Vendor Due Diligence Questionnaire along other information as needed to support those responses. Vendor represents and warrants that all such responses and information were accurate, current and complete, in all material respects. [GDPR 28(1)]

(e) Once per year [upon request], Vendor shall provide Acme with copies of applicable Internal Control Reports. Acme understand that the responses and Internal Control Reports contain Confidential Information of the Vendor, and it shall not disclose the Internal Controls Reports other than to its auditors and advisors in connection with verifying Vendor's compliance with Acme's security and privacy program requirements.

(f) If the Services involve the collection of Personal Information directly from individuals, Vendor will provide the individuals with a clear and conspicuous privacy notice, which notice shall either (i) be Acme's privacy notice, or (ii) be Vendor's privacy notice, provided that such notice must address any legal requirements for such notices in the jurisdictions where it is given, be translated into the languages used in connection with Vendor's interaction with the individuals, and indicate that Vendor is processing the data as a processor on behalf of its clients. All such notices must be approved by Acme.

(g) If the Personal Information will include "protected health information" (or "PHI") as defined in the HIPAA Privacy and Security Rules, Vendor and Acme shall execute an appropriate Business Associate Agreement as required by HIPAA.

(h) If the Personal Information will include EEA Personal Data, Vendor and Acme shall ensure adequate protection for the EEA Personal Data. Each party shall comply with the provisions of GDPR and other Privacy Laws applicable to it, as a "controller" or a "processor" (as defined in GDPR. In the event of any Transfers of EEA Personal Data, the parties shall document adequate protection for the EEA Personal Data using another approved means in accordance with section 4(c) below.

(i) Vendor shall reasonably cooperate with Acme and with its affiliates and representatives in responding to inquiries, incidents, claims and complaints regarding the Processing of the Personal Information or as otherwise needed for Acme to demonstrate compliance with the Privacy Laws applicable to it and to respect individuals' rights under such Privacy Laws. [GDPR 28(3(e) and (f)]

3. <u>Confidentiality and Data Access</u>.

(a) Consistent with the confidentiality provisions of the agreement with Acme, Personal Information is considered Confidential Information of Acme and Vendor must maintain all Personal Information in strict confidence. Vendor may disclose Personal Information to its employees and contingent workers, but only to the extent such individuals require access to the Personal Information to perform the Services. [Some vendors have difficulty with this, particularly if they don't segregate customer data in their systems. While Acme certainly understands that vendors may provide access to multiple workers for the same function (as needed, for example, to ensure coverage

when a particular worker is unavailable), Acme does require Vendors to implement appropriate restrictions on access to its data to minimize the risks of intentional or accidental misuse.]

(b) Prior to allowing any employee or contingent worker to Process any Personal Information, Vendor shall (i) conduct an appropriate background investigation of the individual as permitted by law (and receive an acceptable response), (ii) require the individual to execute an enforceable confidentiality agreement (in a form acceptable to the Acme), and (iii) provide the individual with appropriate privacy and security training. [GDPR 28(3)(b)] Vendor will also monitor its employees and contingent workers for compliance with the privacy and security program requirements.

4. <u>Approvals for Transfers and Subprocessors</u>. [GDPR 28(2), (4)]

(a) Vendor shall not Transfer the Personal Information to any Subprocessors or other third parties unless such Processing is required to perform the Services and it has been explicitly authorized by Acme in writing. [GDPR 28(2)] Vendor shall provide Acme with a list of all such Subprocessors within five (5) days of any request by Acme for such list. [In some cases, a vendor may have outsourced some of its technology functions or system development/maintenance functions to another company or it may house data in a cloud solution. This entity may have access to Acme data in the systems it maintains for our vendor. In this case, Acme will authorize that access provided that the vendor has a written contract with the company that protects the Acme information in an appropriate manner. If a vendor uses subprocessors, these can then be documented using the alternative text.]

[Notwithstanding the preceding paragraph, Acme understand that Vendor has a contractual relationship with [NAME OF COMPANY] pursuant to which [NAME] [provides technology services, hosting, etc. to Vendor]**.** Acme further understands that [NAME] is bound by contract containing terms materially the same as those contained herein that requires it to protect all Vendor information to which it may be exposed. Acme authorizes Vendor to make routine transfers of Personal Information in the normal course of business on its corporate systems to [NAME].

[ALTERNATIVE: Acme approves the following Transfers:

Subprocessor Name Country

[List or Schedule]

Vendor shall ensure that each such Subprocessor has entered into a written contract that contains protections for the Personal Information that are materially the same as the ones contained herein.]

(b) Vendor shall not Transfer the Personal Information across any national borders or permit remote access to the Personal Information from any employee, contingent worker, affiliate, Subprocessor or other third party outside of the country unless Vendor has the prior written consent of Acme for such Transfer. Vendor understands that Acme must authorize all such cross-border transfers, including by use of approved Transfer mechanisms.

[Acme authorizes Vendor to make routine Transfers of Personal Information in the normal course of business on its corporate systems to itself in other countries, including _____, or to other entities in the same group of companies. To the extent that these

Transfers include any EEA Personal Data, Vendor agrees to comply with the provisions paragraph (c) below regarding the Transfers of EEA Personal Data.]

(c) With regard to Transfers of EEA Personal Data, the parties shall assure adequate protection for the EEA Personal Data as follows: [indicate the appropriate option]

_____ The Vendor shall enter into approved EU Standard Contractual Clauses (Processors), a copy of which is attached hereto.

_____ The Vendor has certified its compliance to the EU-US Privacy Shield Program. Vendor shall maintain its certification to the Privacy Shield for so long as it maintains any EEA Personal Data. In the event that EU authorities or courts determine that the Privacy Shield is not an appropriate basis for transfers, Vendor shall promptly execute an approved EU Standard Contractual Clauses (Processors), which shall be incorporated herein upon execution.

_____ The Vendor shall Transfer EEA Personal Data pursuant to its approved set of Binding Corporate Rules for Data Processors.

In the event that EU authorities or courts determine that the Transfer mechanism selected above is no longer an appropriate basis for Transfers, Vendor and Acme shall promptly take all steps reasonably necessary to demonstrate adequate protection for the EEA Personal Data, using another approved mechanism. Vendor understands and agrees that Acme may terminate the Transfers as needed to comply with the EEA Privacy Laws.

5. Information Security Requirements. [GDPR 28(3)(c), GDPR 32]

(a) Vendor shall have implemented and documented appropriate administrative, technical and physical measures to protect Personal Information against accidental or unlawful destruction, alteration, unauthorized disclosure or access. [If Acme has specific security control requirements, add this text (and an annex and then delete any provisions below that are no longer needed. If desired, you could also attach a vendor-prepared security statement.] [Vendor's security program shall contain the minimum standards set out forth in Security Requirements Document, a copy of which is attached hereto.] Vendor will regularly test and monitor the effectiveness of its safeguards, controls, systems and procedures. Vendor will periodically identify reasonably foreseeable internal and external risks to the security, confidentiality and integrity of the Personal Information, and ensure that these risks are addressed.

(b) Vendor shall have implemented and documented appropriate business continuity and disaster recovery plans to enable it continue or resume providing Services (including restoring access to the Personal Information) in a timely manner after a disruptive event. Vendor will regularly test and monitor the effectiveness of its business continuity and disaster recovered plans. At appropriate intervals or as otherwise requested by Acme, Vendor will provide a copy [summary] of its written business continuity and disaster recovery plans to Acme.

(c) If the Processing involves the transmission of Personal Information over a network, Vendor shall have implemented appropriate supplementary measures to protect the Personal Information against the specific risks presented by the Processing. [Sensitive] Personal Information may not be transmitted over any insecure network unless it has been appropriately encrypted.

(d) [Sensitive] Personal Information may not be stored on any portable computer devices or media (including, without limitation, laptop computers, removable hard disks, USB or flash drives, personal digital assistants (PDAs) or mobile phones, DVDs, CDs or computer tapes) unless it is encrypted.

(e) Upon request, Vendor shall provide Acme with information about the Vendor's information security program. Vendor shall also submit its data processing facilities for audit, [at Acme's expense,] [during Vendor's reasonable business hours,] which shall be carried out by Acme (or by an independent auditor designated by Acme) in a mutually-agreeable manner no more than ten (10) day after any such request. Vendor shall fully cooperate with any such audit. In the event that any such audit reveals material gaps or weaknesses in Vendor's security program, Acme shall be entitled to terminate Vendor's Processing of Personal Information until such issues are resolved. [Such audits may occur only once per year; provided however, that Acme may audit at any time in the event of a security breach or suspected material violation by Vendor of its obligations under the Agreement.] [At Acme's expense,] Vendor shall also cooperate with any audits conducted by any regulatory agency that has authority over Acme as needed to comply with applicable law. [GDPR 28(3)(h)]

(f) Vendor will promptly and thoroughly investigate all allegations of unauthorized access to, use or disclosure of the Personal Information. Vendor will notify Acme within 24 [48] hours upon discovery of any Security Breach. This notification must be made as follows: [includes specific notification process, *e.g.,* email Acme security team, call Acme helpdesk.] Vendor shall provide Acme with all information about the Security Breach reasonably needed by Acme to assess its incident response obligations. [GDPR 33]

[If the Security Breach results from either (i) the negligence or misconduct of Vendor (or any Vendor Subprocessor) or (ii) a failure of Vendor to comply with the terms of this Standard or its Agreement with Acme,] Vendor shall bear all costs associated with resolving a Security Breach, including (without limitation), conducting an investigation, engaging appropriate forensic analysis, notifying individuals, regulators and others as required to by law or the Payment Card Industry Data Security Standard, providing individuals with credit monitoring (or other appropriate remediation service), and responding to individual, regulator and media inquiries.

(g) When the Vendor ceases to perform Services for Acme (and at any other time, upon request), Vendor will either (i) return the Personal Information (and all media containing copies of the Personal Information) to Acme, or (ii) purge, delete and destroy the Personal Information. Electronic media containing Personal Information will be disposed of in a manner that renders the Personal Information unrecoverable. [Upon request,] Vendor will provide Acme with an Officer's Certificate to certify its compliance with this provision. If Vendor is required by applicable law to retain any Personal Information, Vendor warrants that it shall (i) ensure the continued confidentiality and security of the Personal Information, (ii) securely delete or destroy the Personal Information when the legal retention period has expired, and (iii) not actively Process the Personal Information other than as needed for to comply with law. [GDPR 28(3)(g)]

(h) Vendor shall carry appropriate insurance to address the risks from its Processing of the Personal Information, including risks of cyber-attacks and security breaches. [Acme shall be named a third party beneficiary of these policies.]

[Add contract boilerplate and signature Lines if this is not part of another contract.]

* * *

Annexes (as needed)

Security Requirements Document

EU Model Contract

HIPAA Business Associate Agreement