SAP U.S. Benefits Administration by Benefitfocus
Supplemental Terms and Conditions

SAP and Customer have entered into an agreement for a subscription to certain SAP products and services ("Agreement") pursuant to which Customer is subscribing to SAP U.S. Benefits Administration by Benefitfocus (the "Cloud Service"). These Supplemental Terms and Conditions ("Supplement") and any modifications to the Agreement made herein apply solely to the Cloud Service and not to any other SAP product or service.

1. CLOUD SERVICE

1.1. The Cloud Service is intended for use with SAP SuccessFactors Employee Central for employee benefits administration for Customer's and its Affiliates' employees. As such, Customer must have a current subscription to SAP SuccessFactors Employee Central as a prerequisite to subscribe to and use the Cloud Service.

1.2. The Cloud Service is only intended for processing data of United States-based employees. If Customer wishes to process data of non-United States based employees, Customer must contact SAP to enter into a separate agreement relating to the processing of personal data of such employees. All data will be processed in data centers located in the United States.

1.3. Implementation services are required to configure the Cloud Service to meet Customer's business needs. These implementation services are not included in the Cloud Service.

2. FEES

The Usage Metric for the Cloud Service is a Flat Fee, plus Users. A User is any individual authorized to access the Cloud Service. The Flat Fee includes 1,500 Users (per User type), and a per-User fee is required for all additional Users.

2.1. **User Types**. Two types of Users are used to calculate the fees for the Cloud Service:

(a) Benefit Eligible Employee. A Benefit Eligible Employee means an employee that is eligible to enroll in at least one benefit type configured within the Cloud Service.

(b) Non-Benefit Eligible Employee. A Non-Benefit Eligible Employee means (i) an employee that is not eligible for enrolling in a benefit configured within the Cloud Service and is provided access to the user communications portal component in the Cloud Service, or (ii) an employee whose data shall be loaded and stored within the Cloud Service solely for the purpose of performing data transmission and/or reporting functions.

2.2 **Add On for Additional Interfaces.** A per User charge is assessed for any Additional Interface. Fees for Additional Interfaces are based on the total number of Benefit Eligible Employees in Customer's subscription to the Cloud Service. An Additional Interface means:

(a) Each Integrated Carrier in excess of six;

(b) For any Integrated Carrier, each group of up to three benefit types per Integrated Carrier that exceeds three; and

(c) Each additional standard payMax payroll integration in excess of one.

2.3 **Add On for the Affordable Care Act (ACA).** A per User charge is assessed for the Add On for the Affordable Care Act (ACA). Add On for the Affordable Care Act fees are based on the total number of Benefit Eligible Employees in Customer's subscription to the Cloud Service, or if Customer has subscribed to both Benefit Eligible Employees and Non-Benefit Eligible Employees, the total number of both. SAP shall provide Customer with the ability to load the applicable data required for the current reporting period within a self-service file upload tool in order to populate the 1094-C and 1095-C Forms, and utilizing the standard Cloud Service file format and specifications. SAP will provide an electronic version of the 1094-C and 1095-C Forms. It is Customer's responsibility to provide the data in the required format as designated by SAP from time to time and communicated to Customer upon request by submitting a support ticket.

3. DATA PRIVACY AND SECURITY.

The Data Privacy and Security – Data Controller to Data Processor Agreement referenced in or attached to the Order Form is superseded by the terms in **Attachment 1** to these Supplemental Terms and Conditions which is incorporated herein by reference.

Attachment 1
To
Supplemental Terms and Conditions
For
SAP U.S. Benefit Administration by Benefitfocus
U.S. Data Protection Agreement

1. DEFINITIONS

1.1 "SAP Affiliates" shall mean any of SAP's affiliates and subsidiaries, meaning a corporation or other entity of which SAP owns, either directly or indirectly, more than fifty percent (50%) of the stock or other equity interests.

1.2 "Data" and/or "data" shall mean any information relating to an identified or identifiable natural or legal person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

1.3 "Service" shall mean any work or service which SAP provides to Customer or its Affiliates which incorporates the terms of this U.S. Data Protection Agreement by reference.

2. PURPOSE OF DATA TRANSFER; OWNERSHIP OF DATA

2.1 SAP will process Data from Customer to provide the Service to Customer and to create aggregate statistics about the use of the Service, which may be used by SAP and its partners to improve the Service.

2.2 As between Customer and SAP, all Data and data carriers provided to SAP from Customer and any copies, reproductions, summaries, analyses or extracts thereof or based thereon, including (without limitation) those made by SAP in performance of its obligations under the Agreement, are the property of Customer and shall be promptly returned to Customer upon any of the following events, whichever is earliest: (i) upon Customer's request; or (ii) upon completion of all tasks for which the respective Data was transferred to SAP; or (iii) upon expiry or termination of the Agreement. Alternatively, where Data and/or data carriers cannot be returned, or if Customer elects so, SAP shall destroy and certify to Customer in writing that he has destroyed all such Data and data carriers which otherwise would have to be returned in accordance with this Section 2.2.

2.3 This Service is only available within the United States and this Data Protection Agreement applies only to transfers of Data within the United States. Prior to any contractual data processing subject to EU Data Protection Directive 95/46/EC, including transfer of personal data outside of the European Union/European Economic Area, the parties agree to execute additional written agreements containing adequate regulations to protect the individuals' privacy and comply with applicable data protection laws.

2.4 To the extent that Customer transfers or provides any Data to SAP, Customer represents and warrants that Customer has collected such Data in accordance with applicable law.

3. ADDITIONAL OBLIGATIONS

3.1 For processing Data, SAP and its subprocessors shall only use personnel who are subject to a binding obligation to observe data secrecy or secrecy of telecommunications, to the extent applicable, pursuant to the applicable data protection law.

3.2 SAP shall ensure that any subcontractors, service providers or other entities processing Data subject to this Data Protection Agreement on behalf of SAP (hereinafter, "subprocessors") are required to have substantially similar protections for Data under this Agreement. SAP remains liable for the compliance of its subprocessors with applicable law. SAP shall reasonably cooperate with Customer in dealing with inquiries and requests relating to SAP's processing of Data within the context of a Service.

3.3 If Customer is a Covered Entity that will provide to SAP, in connection with consuming the Services, Protected Health Information that is subject to protection under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA"), the Health Information Technology for Economic and Clinical Health ("HITECH)" Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 ("ARRA"), Pub. L. No. 111-5 (Feb. 17, 2009) and related regulations, the HIPAA Privacy Rule ("Privacy Rule"), Customer shall notify SAP and the parties agree to execute a Business Associate Agreement.

4. REPORTING OF VIOLATIONS; COMPLIANCE AUDITS

4.1 SAP will promptly report to Customer as soon as commercially feasible (a) any violations or reasonable suspicion that a violation of this Data Protection Agreement has occurred and (b) any actual or a reasonable suspicion of unauthorized access to Data.

4.2 For the production systems which run the Service itself and during the term of the Agreement SAP shall maintain, at its own expense, applicable certifications or audit reports. Unless provided otherwise in a Supplement, SAP engages an internationally recognized independent third party auditor to review the measures in place in protection of the Service(s). Certifications may be based on ISO 27001 or other standards (scope as defined in certificate). For certain SAP Cloud Services, SAP performs regular audits (at least annually) via certified auditors to provide a valid SOC 1 Type 2 (SSAE 16 or ISAE 3402) and/or SOC 2 Type 2 report. Audit reports are available through the third party auditor or SAP, as applicable. Upon Customer's request, SAP shall inform the Customer about the applicable certifications and audit standards available for the Service concerned.

4.3 If SAP fails to perform its audit obligations under Section 4.2 and has not provided sufficient evidence of its compliance after Customer's written request, Customer (or an independent third party auditor on its behalf that is subject to confidentiality obligations consistent with those in the Agreement) may audit SAP's control environment and security practices relevant to Data processed hereunder for Customer once in any twelve (12)-month period, with reasonable prior written notice (at least 60 days unless a data protection authority requires Customer's earlier control under applicable law) and under reasonable time, place and manner conditions.

4.4 Furthermore, (i) following an event set out in Section 4.1 above, or (ii) if Customer has reasonable ground to suspect the non-compliance of SAP with its obligations under this Exhibit, or (iii) if a further audit is required by Customer's data protection authority, Customer (or an independent third party auditor on its behalf that is subject to confidentiality obligations consistent with those in the Agreement) may audit SAP's control environment and security practices relevant to Data processed hereunder for Customer in accordance with applicable law.

4.5 SAP shall reasonably support Customer throughout these verification processes and provide Customer with the required information. Customer shall bear any costs (including SAP's internal resource based on then-current daily professional service rates per SAP's price list) for any efforts on SAP's side exceeding more than 4 hours per year.