This document has been prepared to assist customers and prospects preparing data protection impact assessments (DPIA) or other privacy impact assessments associated with their use of or evaluation of FinancialForce applications.

Note: FinancialForce does not represent or warrant that the information provided in this document will ensure compliance with the General Data Protection Regulation (GDPR) or any other law, the information is provided merely to assist those preparing DPIAs or other privacy impact assessments.

This is based on the Article 29 Working Party Guidance for Data Protection Impact Assessments issued by the European Commission (https://ec.europa.eu/newsroom/document.cfm?doc_id=44137)

The WP29 proposes the following criteria which data controllers can use to assess whether or not a DPIA, or a methodology to carry out a DPIA, is sufficiently comprehensive to comply with the GDPR:	**FF Information**
o a systematic description of the processing is provided (Article 35(7)(a)): ***o nature, scope, context and purposes of the processing are taken into account (recital 90);***	*FinancialForce provides software-as-a-service solutions, including the following applications covered in this document: Financial Management, which enables businesses to automate key finance functions - including accounting, revenue recognition, billing, and payments - in a customer-centric manner; Professional Services Automation, which enables businesses to automate professional services operations, including project, resource, time and expense management; and Human Capital Management, which enables businesses to automate key human resources functions, and which FinancialForce intends to cease providing in 2022 (collectively "FinancialForce Services"). The FinancialForce Services were developed and operate on the Salesforce platform, an industry-leading and mature platform for cloud applications, and benefit from the security and data protection features that the Salesforce platform offers.*
o personal data, recipients and period for which the	*FinancialForce provides the FinancialForce Services to its customers, which may in turn use the FinancialForce Services to store, manage and*

personal data will be stored are recorded;	*process data about and communicate with data subjects. As a data processor, FinancialForce does not know the identities of, or directly communicate with, its customers' data subjects. It is the customer's responsibility, as the data controller, to communicate the details of the processing to its data subjects.* *FinancialForce Services are built on the Salesforce platform. Regardless of which data centres a customer's data is stored in, the Salesforce platform may store in all data centres globally identifying information about customers users for the purposes of operating the FinancialForce Services, such as facilitating the login process and enabling FinancialForce to provide customer support. For more details, please see the FinancialForce Trust and Compliance Documentation.* *Additionally, FinancialForce affiliates and subcontractors across all global regions may access customer personal data to provide support to customers. These entities and their locations are set out in the FinancialForce Trust and Compliance Documentation. Any such access for support purposes is subject to the customer's electronic consent on a case-by-case basis.* *Customers choose how long to retain Customer Data, including personal data, when using the FinancialForce Services. Unless otherwise specified in the contract with the customer or our documentation, FinancialForce does not delete Customer Data, including personal data, during a subscription term, unless the customer instructs FinancialForce to do so. After a customer's contract with FinancialForce terminates, FinancialForce deletes Customer Data, including personal data, in the manner described in the FinancialForce Trust and Compliance Documentation.*
o a functional description of the processing operation is provided;	*FinancialForce provides software-as-a-service solutions, including the following applications covered in this document: Financial Management, which enables businesses to automate key finance functions - including accounting, revenue recognition, billing, and payments - in a customer-centric manner; Professional Services*

	Automation, which enables businesses to automate professional services operations, including project, resource, time and expense management; and Human Capital Management, which enables businesses to automate key human resources functions, and which FinancialForce intends to cease providing in 2022.
o the assets on which personal data rely (hardware, software, networks, people, paper or paper transmission channels) are identified;	*FinancialForce Services are built, and all data submitted to the FinancialForce Services is stored, on the Salesforce platform. Storage locations for personal data submitted to the FinancialForce Services are described in the FinancialForce Trust and Compliance Documentation.*
o compliance with approved codes of conduct is taken into account (Article 35(8));	*FinancialForce does not submit to any codes of conduct.*
o necessity and proportionality are assessed (Article 35(7)(b)): **o measures envisaged to comply with the Regulation are determined (Article 35(7)(d) and recital 90), taking into account:** **o measures contributing to the proportionality and the necessity of the processing on the basis of:** **o specified, explicit and legitimate purpose(s) (Article 5(1)(b));** **o lawfulness of processing (Article 6);** **o adequate, relevant and limited to what is necessary data (Article 5(1)(c));** **o limited storage duration (Article 5(1)(e));**	*With respect to data submitted to the FinancialForce Services, FinancialForce acts as a data processor. With respect to data collected by FinancialForce in its other business activities (such as, for example, sales, marketing and professional services activities and management of its employees), FinancialForce processes data both as a data controller and a data processor.* *The FinancialForce Services allow customers to manage the personal data they maintain in the FinancialForce Services, including in response to data subject requests. To the extent a customer needs FinancialForce's assistance to respond to a Data Subject, FinancialForce will provide assistance as described in section 3 of our Data Processing Addendum.* *When providing the FinancialForce Services, FinancialForce is a data processor for the customer and the lawful basis for processing is the performance of the contract with the customer.* *FinancialForce sets out protections for personal data in our contracts with customers. Contractual documents containing protections for personal data include (1) a master subscription agreement between FinancialForce and the customer; and (2) a Data Processing Addendum, which can be added to the contract (if not already included) by downloading from here.*

o measures contributing to the rights of the data subjects: **o information provided to the data subject (Articles 12, 13 and 14);** **o right of access and to data portability (Articles 15 and 20);** **o right to rectification and to erasure (Articles 16, 17 and 19);** **o right to object and to restriction of processing (Article 18, 19 and 21);** **o relationships with processors (Article 28);** **o safeguards surrounding international transfer(s) (Chapter V);** **o prior consultation (Article 36).**	*FinancialForce commits in clause 5.1 of the Data Processing Addendum to ensure it has contracts in place with its suppliers. See information on sub-processors in FinancialForce Trust and Compliance Documentation.* *Customers choose how long to retain Customer Data, including personal data, when using the FinancialForce Services. Unless otherwise specified in the contract with the customer or our documentation, FinancialForce does not delete Customer Data, including personal data, during a subscription term, unless the customer instructs FinancialForce to do so. After a customer's contract with FinancialForce terminates, FinancialForce deletes Customer Data, including personal data, in the manner described in the FinancialForce Trust and Compliance Documentation.* *FinancialForce Services are built on the Salesforce platform. The Salesforce platform has data centers in the EU; however, Salesforce does not guarantee that personal data of FinancialForce's customers (including its EU-based customers) will be stored exclusively in EU data centers. In addition, regardless of which data centres a customer's data is stored in, the Salesforce platform may store in all data centres globally identifying information about customers users for the purposes of operating the FinancialForce Services, such as facilitating the login process and enabling FinancialForce to provide customer support. For more details, please see the FinancialForce Trust and Compliance Documentation.* *Additionally, FinancialForce affiliates and subcontractors across all global regions may access customer personal data to provide support to customers. These entities and their locations are set out in the FinancialForce Trust and Compliance Documentation. Any such access for support purposes is subject to the customer's electronic consent on a case-by-case basis.* *In addition, FinancialForce will transfer personal data outside of the EU utilizing the EU Standard Contractual Clauses. For more information about this transfer mechanisms please review our Data Processing Addendum.*

o risks to the rights and freedoms of data subjects are managed (Article 35(7)(c)): **o origin, nature, particularity and severity of the risks are appreciated (cf. recital 84) or, more specifically, for each risk (illegitimate access, undesired modification, and disappearance of data) from the perspective of the data subjects:** **o risks sources are taken into account (recital 90);** **o potential impacts to the rights and freedoms of data subjects are identified in case of events including illegitimate access, undesired modification and disappearance of data;** **o threats that could lead to illegitimate access, undesired modification and disappearance of data are identified;** **o likelihood and severity are estimated (recital 90);** **o measures envisaged to treat those risks are determined (Article 35(7)(d) and recital 90);** **o interested parties are involved:**	*FinancialForce customers choose what data to submit to the FinancialForce Services. FinancialForce provides online software-as-a-service solutions for financial management, professional services automation, and human capital management. FinancialForce's customers typically use the FinancialForce Services to manage their own businesses, interact with their own customers and employees, and manage the information surrounding those interactions. As the data controller, the FinancialForce customer should determine its specific purpose for processing personal data in the FinancialForce Services. FinancialForce processes personal data to offer the FinancialForce Services pursuant to the terms agreed in its contract with the customer.*

o the advice of the DPO is sought (Article 35(2)); **o the views of data subjects or their representatives are sought, where appropriate (Article 35(9)).**	