This document provides a broad overview of Data Protection Impact Assessments under the EU General Data Protection Regulation (GDPR) and does not provide legal advice. We urge you to consult with your own legal counsel to familiarize yourself with the requirements that govern your specific situation.

Salesforce's Trust Commitment

At Salesforce, trust is our #1 value, and nothing is more important than the protection of our customers' data. As part of that commitment, we take privacy very seriously. This includes putting privacy at the forefront of our product development process and as a driver of innovation. This approach to privacy and data protection is called "privacy by design" or "data protection by design."

GDPR and Data Protection Impact Assessments

Privacy by design has existed in the privacy world for some time but this principle has now been enshrined in law under the EU General Data Protection Regulation (or "**GDPR**").

Under the GDPR, Salesforce customers (or "controllers" as they are referred to in the GDPR) have a general obligation to ensure that privacy by design occurs in practice. This means actively considering privacy and data protection concepts in the early stages of any project and throughout its lifecycle, as well as designing projects, processes, products or systems with privacy in mind. The key objective for privacy by design is to implement data protection principles and integrate the necessary safeguards into data processing in order to meet the requirements of the GDPR and protect the rights of individuals (Article 25 GDPR).

Controllers can demonstrate their compliance with privacy by design in a number of ways, but one way to do so is by undertaking a data protection impact assessment ("**DPIA**"). DPIAs are assessments that evaluate new projects, processes, products or systems and aim to flag up privacy and data privacy issues at the outset and at critical stages of any initiative involving personal data. The aim of conducting a DPIA is to identify, and then remedy or address, the origin, nature, particularity and severity of any risk posed to individuals by an initiative involving their personal data. They should also consider the scope, context and purposes of the processing, the sources of the risk and the measures, safeguards and mechanisms envisaged for mitigating that risk.

Under the GDPR, DPIAs are mandatory in certain "high risk" circumstances, which are further described below, but the European Data Protection Board (made up of representatives from each of the European supervisory authorities) generally recommends DPIAs as a useful compliance tool that is helpful in demonstrating privacy by design.

DPIA FAQ

When is a DPIA mandatory?

The GDPR requires controllers to carry out a DPIA where a processing activity is using new

technologies and is likely to result in a “high risk to the rights and freedoms" of individuals (Article 35.1 GDPR). While the GDPR does not specify what constitutes a "high risk" to individuals, it does provide a few examples of when a DPIA is required, which may serve as guidance (Article 35.3 GDPR). This includes:

- Systematic and extensive processing activities: The GDPR states that a DPIA must be conducted where systematic and extensive processing activities (including profiling) are conducted on personal data where decisions based on that processing have legal effects (or similarly significant effects) on individuals. This includes processing which leads to a decision being made that prevents an individual from accessing a particular product or service, or which would determine the price at which an individual can purchase a product or service.

- Large amounts of sensitive personal data: The GDPR states that a DPIA must be conducted where processing involves large amounts of sensitive personal data (or “special categories of personal data” as it is defined under the GDPR) and personal data relating to criminal convictions. This includes where an organization is processing a considerable amount of personal data that affects a large number of individuals and involves a high risk to their rights and freedoms, such as a hospital processing genetic health data of its patients.

- Systematic monitoring of public areas: The GDPR states that a DPIA must be conducted where processing involves systematic monitoring of a publicly accessible area on a large scale, such as the use of a camera system to monitor highways and the use of an intelligent video analysis system to automatically recognize license plates.

If a DPIA is required, it should be carried out before processing starts.

Is conducting a DPIA useful even when it is not required by law?

Yes. At Salesforce, we believe that conducting a DPIA is a helpful part of an overall privacy program to help identify privacy risks, document compliance with applicable laws and internal policies, and ensure customer trust.

What information should be collected as part of a DPIA?

The GDPR provides some details about what controllers should include in their DPIAs (Article 35.7 GDPR), including:

- a detailed description of the project, process, product or system and its purpose/s. If applicable, it should also set out what “legitimate interest” is being pursued by the controller;

- an assessment of the necessity and proportionality of the processing in relation to the purpose/s of the data;

- an assessment of any risks to the rights and freedoms of individuals; and

- any measures to be put in place to address the risks to individuals, including security measures, and to demonstrate compliance with the GDPR.

The GDPR provides controllers with a certain level of flexibility to determine the structure and form of the necessary DPIA in order to best fit the needs of the organization. There are a number of different methodologies available regarding how best to approach a DPIA. The European Data Protection Board also encouraged the development of sector-specific DPIA frameworks that focus on the privacy considerations and threats to particular industries.

What key elements should be included in a DPIA?

It is likely that many of our customers will either undertake either a mandatory DPIA or choose to prepare a voluntary one as a matter of best practice Those customers who undertake DPIAs will need to undertake a detailed assessment of the following issues:

- **Data Processing Principles:** The GDPR sets out a number of principles for which a controller is responsible for complying. Additionally, the controller is also responsible for being able to demonstrate how it complies with these principles. These include that personal data is: (i) processed lawfully, fairly and in a transparent manner; (ii) collected for specified, explicit and legitimate purposes; (iii) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed; (iv) accurate and, where necessary, kept up to date; (v) kept for no longer than is necessary; and (vi) processed in a manner that ensures appropriate security (Article 5 GDPR).

- **Lawfulness of Processing:** Under the GDPR, processing of personal data is only lawful if one of the grounds set out in the GDPR applies; the key ones include: (i) with consent; (ii) necessary for the performance of a contract to which the data subject is a party; and (iii) necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject (Article 6 GDPR).

- **Nature of the Personal Data:** Under the GDPR, certain personal data is subject to more protection. This is called “special categories of personal data” and personal data relating to criminal convictions and offenses. Special categories of personal data are defined as 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 (Articles 9 & 10 GDPR).

- **Individuals' Rights**: Under the GDPR, data subjects' rights (which exist under the current law) have been expanded and reinforced (Articles 16 - 22 GDPR). These include the right to "be forgotten" and the right to data portability in certain circumstances.

- **Security:** The GDPR requires controllers and processors, or those entities that process personal data only the controller's instructions (e.g. Salesforce as processor), to implement appropriate technical and organizational measures to keep personal data secure (Article 32 GDPR).

- **Third Parties / Vendors**: The GDPR requires controllers to only engage processors providing "sufficient guarantees" to implement appropriate security measures and for these guarantees to be documented in a contract (Article 28 GDPR).

- **International Data Flows**: In the event that personal data is transferred outside the European Economic Area ("**EEA**"), the GDPR requires controllers and processors to put measures in place to guarantee that the personal data transferred is adequately protected. The GDPR recognises a number of legal mechanisms (e.g. EU standard contractual clauses, BCR for Processors, EU Commission adequacy decisions, etc.) for legally transferring personal data outside of the EEA.

- **Data Protection by Design & Data Protection by Default**: The GDPR requires controllers to implement appropriate technical and organisational measures to implement the data protection principles and introduce effective safeguards. It also requires controllers to ensure that, by default, only personal data which are necessary for each specific purpose of the processing are processed (Article 25 GDPR).

- **Transparency:** The GDPR requires controllers to be transparent about the processing operations to their data subjects. They must provide notice of the processing operations to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language (Article 12).

- **Accountability:** The GDPR includes a number of accountability obligations, of which DPIAs are one. Others include the appointment of a data protection officer in certain circumstances (Article 37 GDPR) and the creation of records of processing activities (Article 30 GDPR), among others.

How can Salesforce's services help with the DPIA requirements?

To the extent that a customer's DPIA involves an assessment of the Salesforce services, the customer can leverage the DPIAs available at www.salesforce.com/privacy.