This document discusses in general terms 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.

White Paper: GDPR Key Facts

At Salesforce, Trust is our #1 value and the protection of our customers’ data is paramount. We know that many organizations have questions about the GDPR and their obligations under the GDPR. To help you on your compliance journey, we have outlined a few of the notable provisions of the GDPR below.

What is the GDPR?

The EU General Data Protection Regulation (“GDPR”) is a comprehensive data protection law that updates EU data protection laws to strengthen the protection of “personal data” (any information relating to an identified or identifiable natural person, so called “data subjects”) in light of rapid technological developments, the increasingly global nature of business and more complex international flows of personal data. It puts in place a single set of rules, directly enforceable in each EU member state. The GDPR took effect on May 25, 2018.

Does the GDPR affect my organisation?

If you are processing personal data in the context of an organisation established in the EU, the GDPR applies to you, regardless of whether you are processing personal data in the EU or not. “Processing” means any operation performed on personal data, such as collection, storage, transfer, dissemination or erasure.

If you are not established in the EU, the GDPR applies to you if you are offering goods or services (whether paid or free) to EU data subjects or monitoring the behavior of EU data subjects within the EU. Monitoring can be anything from putting cookies on a website to tracking the browsing behavior of data subjects to high-tech surveillance activities.

Under European data protection laws, organisations processing personal data are divided into “Controllers”, or the entities which control the personal data, and “Processors”, the entities that process personal data only on the instructions of the Controllers. The GDPR applies to both Controllers and Processors.
**How does the GDPR change the former EU data protection laws?**

The GDPR changed former EU data protection laws in several ways:

1. **Expanded definition of “personal data”:** The GDPR expands and clarifies the concept of personal data. While the basic concept of personal data largely remains the same, the GDPR makes it clear that location data and online identifiers, such as IP addresses, are considered personal data. The GDPR also expands the concept of “sensitive personal data,” which is more highly regulated, to include genetic data and biometric data.

2. **Expanded and new rights for EU individuals:** The GDPR provides expanded rights for EU data subjects such as:
   - **Deletion:** This right is sometimes referred to as the “right to be forgotten”. The data subject has the right to require that the Controller erase personal data about him or her in certain conditions, including if the personal data is no longer necessary for the original purpose of the processing or if the data subject withdraws consent for the processing.
   - **Restriction:** Under the GDPR, a data subject has the right to obtain from a Controller a restriction on the processing of personal data in certain circumstances, including if the data subject contests the accuracy of the personal data. A restriction on processing means that the data may be stored, but cannot be further processed.
   - **Portability of personal data:** Data subjects also now have the right, in certain circumstances, to receive the personal data that they have provided to a Controller in a structured, commonly used and machine-readable format. Salesforce’s [data processing addendum](#) reflects these expanded and new rights.

3. **Security measures:** The GDPR requires Controllers and Processors to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks presented. At Salesforce, we have robust security measures in place. For some of our services, we have security certifications including the International Organization for Standardization (ISO) 27001 and 27018 standard, the American Institute of CPAs’ (AICPA) System and Organization Controls (SOC) reports, the Payment Card Industry Data Security Standards (PCI DSS), the TÜV Rheinland Certified Cloud Service, TRUSTe Certified seal, and the UK Cyber Essentials Scheme, among others. For further details about our security measures in respect of specific services, please see our [Trust and Compliance](#) documentation.

4. **Breach notification:** The GDPR requires organizations to report certain personal data breaches to the relevant supervisory authority, and in some circumstances, to the affected data subjects. Controllers must notify the relevant supervisory authority “without
undue delay” (and where feasible, within 72 hours of having become aware of it), unless the breach is not likely to present any risk to the rights and freedoms of the data subjects concerned. If circumstances require it, Controllers may also be required to communicate the data breach to data subjects. Processors, for their part, are required to notify Controllers “without undue delay” after becoming aware of a personal data breach. Salesforce’s data processing addendum reflects this new obligation.

5. **Data Protection Impact Assessments**: Where certain processing is likely to be classified as “high risk” to data subjects, the Controller may be required to carry out a data protection impact assessment identifying the impact of the proposed processing operations on the personal data. Salesforce’s data processing addendum reflects this obligation.

6. **International transfers**: European data protection laws restrict the transfer of personal data outside the EU unless there are appropriate safeguards in place to protect that data. The GDPR continues to recognize current mechanisms (e.g., EU standard contractual clauses, EU Commission adequacy decisions, etc.) for legally transferring personal data outside of the EU. The GDPR also formally recognizes Binding Corporate Rules (“BCRs”), a set of company-specific, group-wide data protection policies approved by European supervisory authorities to facilitate transfers of personal data from the EU to other countries. In November 2015, Salesforce became the first top 10 software company in the world to achieve approval for its processor BCRs from the European supervisory authorities.

7. **Consent**: Consent is subject to additional requirements under the GDPR. The GDPR defines consent as “any freely given, specific, informed and unambiguous indication of a data subject’s wishes through a statement or clear affirmative action.” The concept of consent is used throughout the GDPR as a means to legitimize certain processing activities from a legal perspective.

8. **Transparency**: The GDPR requires that Controllers provide data subjects with information about their processing operations at the time when personal data is collected. This information includes the identity and contact details of the Controller, the contact details of the data protection officer (if relevant), the purposes and the legal bases for the processing of the personal data, the recipients of the data and a number of other fields to ensure that the personal data is being processed in a fair and transparent manner. In addition, Controllers are required to provide information to data subjects even in circumstances where the personal data has not been obtained directly from the data subject.

9. **Profiling**: The GDPR introduces the concept of “profiling” or any form of automated processing that uses personal data to evaluate personal aspects and in particular to analyse or predict aspects relating to an individual’s performance at work, economic
situation, health, personal preferences, interests, reliability, behaviour, location or movements. Data subjects must be informed of the existence of profiling and any consequences of the profiling.

10. **Enforcement**: Fines for non-compliance under the GDPR can be substantial. Supervisory authorities have a number of enforcement powers under the GDPR, including the ability to fine organizations up to €20 million or 4% of annual global turnover, whichever is higher. These are maximum fines and it remains to be seen how supervisory authorities will use these enforcement powers.

11. ‘**One Stop Shop**’: Under the GDPR, organizations that are established in more than one EU member state or are processing personal data affecting data subjects in more than one EU country have greater clarity about their supervising data protection authority.

**How does Salesforce assist customers in complying with their obligations under the GDPR?**

Salesforce views the GDPR as an opportunity to deepen our commitment to data protection. Compliance with the GDPR requires a partnership between Salesforce and our customers in their use of our services, and Salesforce is dedicated to helping our customers on their GDPR compliance journey. We have made enhancements to our products, contracts, and documentation to help support both Salesforce's and our customers' compliance with the GDPR. Check out our [privacy website](#) for more information.

**Where can I find out more information?**

Take our "EU Privacy Law Basics" Trailhead module or review our [GDPR: Fiction versus Fact](#). Additional information about the GDPR is available on the official [GDPR website of the EU](#).