Privacy and Ethical Use Principles Guiding our COVID-19 Response

As the COVID-19 pandemic permeates all aspects of our world, we all have a responsibility to do our part. Just as our frontline responders, medical professionals, and essential workers are helping to guide us toward recovery – we recognize that technology can also play an important role in slowing the spread of disease and helping restore our communities.

As we move forward, we have an opportunity to lead by building responsible technology solutions that protect and empower the communities most impacted by this crisis. When we design with our most marginalized in mind, and with the intention to protect individuals' privacy and promote public health, we can contribute to uplifting our entire society.

At Salesforce, our values – trust, innovation, customer success and equality – are our compass, guiding us especially in difficult times. Through this lens, we developed ethical use and privacy principles to inform our approach to responding to the increasing and dynamic COVID-19 challenges and needs.

We share these principles in the spirit of transparency and accountability – and in the hopes our partners, customers, and community can reference them as they build their own solutions.

No matter how good a tool is, people won't use it unless they trust it. Technology developed with human rights and civil liberties top of mind will help drive greater adoption, and ultimately be far more successful in helping the world recover.

Protect human rights and equity.

Solutions should not adversely affect already vulnerable populations, and the underserved should be actively considered as part of the design process.

Considerations:

- Involve advocates, experts and representatives of affected populations in the development of solutions.
- Take steps to uncover and address the risk of bias or discrimination in datasets.
- Ensure the solution does not exclude users – especially those who are already vulnerable – or deny essential services. (For example, ensure your solution incorporates accessibility standards and supports multiple languages.)

Honor transparency.

Trust starts with transparency. Solutions should give individuals timely, accessible, and easily understandable notice of how their data is being collected and used, how their data is protected, and their rights to control the use of that data.

Considerations:

- Develop tools that facilitate making clear to users how data is collected, used and disclosed.
- Ensure that your solution uses data only for purposes clearly disclosed to users at the outset.

- Build features that allow for timely and accurate responses to individuals seeking to exercise their privacy rights.
- Clearly explain any use of artificial intelligence.

Minimize data collection.

Collect and retain only the data that is essential for a solution to be effective.

Considerations:

- Clearly formulate the purpose of the proposed solution, then design the solution so that it collects and retains only the data that is necessary for those purposes.
- Document the datasets or fields required to effectively operate the solution, then challenge whether they are objectively essential for the solution's desired purposes.
- Anonymize or aggregate your data or datasets wherever possible.

Take a long-term approach.

The pandemic will eventually come to an end, but technology solutions, the data collected through those solutions, and their implications may have a longer impact. Solutions should only retain data as long as is necessary for the purposes for which it was collected.

Considerations:

- Enable the solution or its users to immediately and securely delete the data once it is no longer necessary for the solution's purposes (especially when the crisis has ended, if not sooner).
- Build in functionality so data that is only needed for limited functionality can be used in a timely fashion and securely deleted rather than storing the data for the entire duration of the solution or its development.

Ensure the security of data.

Solutions should include protections to secure any collected data.

Considerations:

- Limit access to any datasets stored within the solution to a clearly defined set of individuals with appropriate access permissions on a 'need to know' basis.
- Implement safeguards to protect data against misuse, consistent with industry standards like ISO, the NIST Cybersecurity Framework, etc.

We are learning together.

The situation is rapidly changing and solutions will vary by context. We are learning alongside our partners and will evolve our approach with our learnings. What if I have additional questions? Please reach out to your dedicated account executive or partner account manager who will be able to help with any follow up questions that you may have.

We also have developed resources to help teams build technology responsibly. Take a look:

Trailhead: Learn Privacy and Data Protection Law
Trailhead: Ethics by Design
Trailhead: Responsible Creation of Artificial Intelligence
Trailhead: Security Basics
Trailhead: Get Started with Web Accessibility

Disclaimer:

This document 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 (including requirements around the use of specific technology solutions and the collection and use of personal information).