June 13, 2020

Salesforce is pleased to provide this submission to the public consultation of the European Commission on the White Paper "On Artificial Intelligence - A European approach to excellence and trust". Salesforce welcomes discussion on this important topic.

AI has the potential to generate improved efficiency and productivity, bring solutions to complex problems through unique insights from vast amounts of data, and help users focus on the important tasks. Salesforce upholds the highest standards of technology and human integrity through its values, it nonetheless acknowledges the ethical concerns that come with the accelerated use of AI at large, including the potential to strengthen discrimination and weaken human rights. Companies that develop AI have a responsibility to ensure it complies with essential ethical and safety principles, and the regulatory framework should provide the right incentives for doing so.

Salesforce

Salesforce is a provider of software-as-a-service ("SaaS") and platform-as-a-service ("PaaS") offerings, and a global leader in cloud enterprise software for customer relationship management (CRM). Founded in 1999, Salesforce enables organisations of all sizes and in every industry to take advantage of powerful technologies like cloud, mobile, social, voice, and artificial intelligence, to connect to their customers in new, smarter ways.

Salesforce is committed to a set of core values — **trust, customer success, innovation, and equality of every human being.** Since we were founded, we have pioneered the 1-1-1 philanthropic model and we give 1% of our employee time, 1% of our product and 1% of our equity back to communities around the world.

Salesforce has been operating in Europe since 2000. According to IDC, our ecosystem of customers, partners and developers is expected to help create 493,000 jobs in Europe and contribute over $242 billion to the continent's GDP growth from 2019 through 2024.

Salesforce and Artificial Intelligence

Salesforce's AI capability, called "Einstein", is built into the Salesforce Platform, and is designed to add artificial intelligence in Salesforce services, democratising the power of AI for every Salesforce user. Salesforce Einstein enables organisations of all sizes to deliver smarter, more personalised customer experiences by automatically discovering relevant insights, predicting future behaviour, proactively recommending best next actions and automating tasks. Salesforce is delivering more than 10 billion AI-driven predictions to its customers every day. Those predictions have the power to improve and transform the way societies live and work.

At Salesforce, we have determined that the ethical use of technology must be clearly addressed. Technology is not inherently good or bad. It's what we do with it that matters. That is why we have made ethical use a strategic initiative at Salesforce through the establishment of the **Office of Ethical and Humane Use of Technology**. The office works across product, law, policy, and ethics to develop and implement a strategic framework for the ethical and humane use of technology across our company. Through this work, we have established a set of guiding principles on the ethical use of technology that safeguards such rights as human rights, data privacy, and human safety. Most recently, we developed ethical use and privacy principles to inform our approach to responding to COVID-19 challenges and needs.

Turning to AI, we believe its tremendous benefits should be accessible to everyone. But we also have an

important responsibility to ensure that AI is safe and inclusive for all. At Salesforce, we are committed to providing our employees, customers, and partners with the tools they need to develop and use AI safely, accurately, and ethically. **Our commitment to ethical AI consists of the following principles:**

- **Responsible:** To safeguard human rights and protect the data we are entrusted with, we work with human rights experts, and educate, empower and share our research with customers and partners to enable them to use AI responsibly. We respect laws and regulations. We strive to adhere to the highest security and safety protocols.
- **Accountable:** Accountability to customers, partners and society is essential. Independent feedback should be sought for continuous improvement of practices and policies and work to mitigate against harm to customers and consumers. We seek stakeholders' feedback, take guidance from our Ethical Use Advisory Council, and conduct our own data science review board.
- **Transparent:** Our customers should be able to understand the "why" behind each AI-driven recommendation and prediction so they can make informed decisions, identify unintended outcomes, and mitigate harm. We strive for model explainability and clear usage terms, and ensure customers control their own data.
- **Empowering:** AI is best utilised when paired with human ability, effectively augmenting people and enabling them to make better decisions. Accessible AI promotes growth and increased employment, and benefits society as a whole.
- **Inclusive:** AI should respect the values of all those impacted, not just of its creators. To achieve this, we test models with diverse data sets, seek to understand their impact, and build inclusive teams.

Lastly, we believe that promoting responsible industry adoption of AI is key. For this reason, Salesforce has engaged in a number of policy processes around the world aimed at establishing frameworks to ensure responsible adoption. These include the following:

- We have partnered with the World Economic Forum on their government procurement guidelines for artificial intelligence (AI), which have been piloted with the government of the United Kingdom.
- We have extensively engaged with Singapore's Personal Data Protection Commission (PDPC) on their Model AI Governance Framework.
- We have urged the United State's National Institute of Standards and Technology (NIST) to begin work on the establishment of a framework for AI.

In the following pages, we share some more detailed comments on a number of the points raised in the White Paper:

General remarks:

1. We support the Commission's intention to focus any future regulatory action on high-risk applications of AI, taking into account the context in which the technology is used. **Principles-based and future-proof legislation** that leaves no room for uncertainty with regard to its interpretation should be the desired outcome. A **clear and targeted definition of "high risk"** will help achieve this outcome, as will a clear scoping of **the specific context in which an AI application is used** when assessments of risk are made.

2. We call for any future regulation to take into account the different considerations that appear in the Business to Consumer (B2C) v. Business to Business (B2B) contexts, in particular with regard to liability. The Commission rightly acknowledges in its White Paper that "each obligation should be addressed to the actor(s) who is (are) best placed to address any potential risks" (page 22). **In the B2B environment, contractual arrangements between the AI developer and the AI user clearly allocate liability among parties**, and can be further tailored to cater to the different contexts in which the AI is used. The AI user ultimately controls when to use the products, which data is submitted to the AI and when, how the AI is configured, and, most critically, how the resulting predictions are used. It is the AI user, and not the AI

developer, that knows what has been disclosed to the affected individual, and what the risk of harm is to the affected individual.

3. Introducing new mandatory rules for high-risk applications could go some way in alleviating the concerns identified in the questionnaire. However, what will really make a difference is **continuous education and a cultural shift within the whole value chain towards the ethical and responsible design and adoption of AI**. As with other European regulations, e.g. the GDPR, the new rules should not be a rigid list of requirements that stakeholders need to "tick off", often without understanding what they're required to do. The guidelines of the High-Level Expert Group on Artificial Intelligence should be taken into account in any future regulatory action and we suggest that the Group retain a **permanent advisory role to the European Commission** as new rules on AI are being developed.
4. The EU has already developed a robust body of law covering many of the concerns presented in the White Paper. This, in combination with the fundamental values of the European Union, already provide a **strong foundation for the ethical behaviour of technology companies**. We would encourage the Commission to make a thorough assessment and presentation of EU legislation currently applicable to AI in the form of an **"AI rulebook"** (similar to the cloud rulebook the Commission announced in its Data Strategy). This would be of great benefit to researchers, SMEs, AI developers and users alike, as it would facilitate compliance. It would also be a useful tool to the Commission as it contemplates the potential need for further regulatory action.
5. Lastly, we call on the Commission to recognise and embrace values-driven businesses striving for ethical, responsible, and inclusive AI. **Respect for European values in addition to compliance with European rules can guarantee the development and uptake of ethical AI in Europe.**

Comments on "An ecosystem of excellence":

- Skills:
  - Emerging technologies like AI are creating a massive skills gap across Europe, which in turn adds to fears of a widening inequality gap. Per the Commission's 2020 DESI report, 42% of the EU population has an insufficient level of digital skills. JRC's technical report on Academic offer and demand for advanced profiles in the EU (2019) shows that most Member States are facing shortages of ICT professionals and technicians, while the current education offer of specialised higher education programmes is limited and not equally available in all Member States. Therefore, there is a clear need for these skills to become an integrated part of the school curricula.
  - It is equally important for governments and businesses to work together to upskill the workforce. We recommend to the Commission and Member States to support public and private initiatives that aim to close the AI skills gap and will allow an increasingly specialised workforce to emerge. Today, an increasing number of businesses offer training programmes aiming to upskill Europeans. For instance, Salesforce offers Trailhead, a free online learning platform that gives the opportunity to all to acquire technical knowledge into a Salesforce role (e.g. administrator, coder, or marketer) and at their own pace. At the moment there are more than 2 million people globally learning new skills on our platform. In Europe, we work with partners including educational institutions and apprenticeship programmes to bring these trainings to the wider community, with a focus on underrepresented groups.
  - Any AI skills initiative should also include a strong focus on topics such as ethics/moral philosophy and user research/ethnography. Education within these fields is necessary for everyone involved in the life cycle of AI development and use to better understand the impact of the AI systems on society and individual groups and thus create more responsible AI. AI developers, researchers, designers, administrators and users as well as regulators and public authorities should be educated on topics like fairness, accountability, and transparency/explainability of AI.

- The importance of partnerships with the private sector and the adoption of AI in the public sector:

- Public-private partnerships should be further encouraged and should remain open to private enterprises that respect European laws and fundamental values, and have a strong track record in trust and operational excellence, irrespective of where their headquarters might be located.
- On the adoption of AI in the public sector, we would like to point out the WEF project on AI procurement guidelines for the public sector. Similar guidance at the EU level could be useful for the further uptake of AI in the public sector. We would suggest that the results of the sector dialogues with the public sector mentioned in the White Paper be reflected in each country's AI Strategy. Modernisation of the public sector through the use of AI should be an express goal of national IT transformation plans. The Commission could support and integrate such guidance in the implementation of its own Digital Strategy.

Comments on "An ecosystem of trust":

- Possible adjustments to existing EU legislative framework relating to:
  - The European Commission identifies a number of regulations in the White Paper that are currently applicable to AI. We would encourage the Commission to undertake a thorough analysis of the existing rules and their effective application to the AI context (or any gaps therein), before suggesting additional regulation.
  - Europe should avoid the "regulatory patchwork" phenomenon that threatens to create further confusion in the market and consequently delay the development and adoption of AI. Conversely, codifying existing rules into an "AI rulebook" and issuing relevant guidance would help all stakeholders have a clearer understanding of their rights and obligations.

- The scope of a future regulatory framework:
  - We support the Commission's focus on high-risk applications. We would also like to reiterate the importance of taking into account the specific context in which an AI application is used when making the assessment of what constitutes a high-risk application. For instance, in a B2B environment, the same application will be used in many different ways from different customers. Some of them will be higher risk than others. Therefore, the regulator should look at the specific use case when determining the level of the risk, rather than the technology solution.
  - We support the two cumulative criteria for what constitutes a high-risk application as set out in the White Paper. However, we believe that this definition needs to be as tightly and clearly phrased as possible to prevent market confusion and legal uncertainty. We would also encourage the Commission to align the 2nd functional criterion to the Product Liability Directive, which applies to damage caused by death or personal injuries or caused to private property (as opposed to "risk of injury, death or significant material or immaterial damage" as phrased in the White Paper, which could increase legal uncertainty).
  - A third criterion added to the definition of high-risk applications could be whether the application fully replaces human activity (in which case the application should be more closely scrutinised), compared to applications that simply help augment human capability and would likely create lower risk. For example, medical AI that double-checks an independently-formed physician's recommendations, and could raise a red flag, could be treated differently than AI that was meant to supplant a physician's recommendations. It is important to take into account the inherent risks in the status quo situation with no AI involvement, and whether the particular application of AI heightens these risks (either for individuals or the population), not merely whether "significant risks are likely to arise."

- Regarding the proposed mandatory requirements:
  - Quality of training data sets: In the B2B context, the organisation developing the AI tool can control the quality of the data sets it uses to build or test its own AI system. However, most B2B AI systems operate in part on the customer's data as well, and may operate differently for every customer. The

B2B organisation developing the AI tool cannot control the quality of the datasets its customers use once they start using the AI product or service, as this data belongs to the customer. This should be understood similarly to the data processor/data controller distinction we meet in the GDPR. What the AI developers can do in these instances is provide tools to their customers to enable them identify potential bias in their data sets. For instance, Salesforce offers a feature called “Sensitive Fields” (formerly called Protected Fields). This allows users to flag sensitive variables in the data set (e.g., age, race, gender) and then our tool "Einstein Discovery" will find all of the variables that are highly correlated with the sensitive variables. For example, zip code is usually highly correlated with race and therefore a proxy for race in AI modelling. Users can then decide if they want to "protect" (not include) those variables in the model. It would also be useful to clarify how companies could "take reasonable measures aimed at ensuring that such subsequent use of AI systems does not lead to outcomes entailing prohibited discrimination" (page 19 in the White Paper) in light of the heightened requirements to handle sensitive data under Article 9 of GDPR without requiring the explicit consent of every data subject, which is difficult in practice and can skew datasets.

- The keeping of records and data: It would be useful if the Commission specified the level of detail required. This requirement (as any other potential mandatory requirement) should be in full alignment with existing laws and regulations, including the GDPR, intellectual property rules, etc. It would be helpful if the Commission clarified how these requirements will interact with the GDPR, including the Right to be Forgotten and Data Minimisation, and other data privacy laws.
- Information on the purpose and the nature of AI systems: This is a very important point, as AI developers would normally not want their users/customers to ignorantly apply AI for use cases it wasn't designed for, especially in high-risk cases. However, similar to our point on the quality of training data sets, in the B2B context the organisation that develops the AI cannot proactively monitor the way its customers are using the AI. Customers control what predictions are made, and more critically, how these predictions are used within their organisation. In these cases, AI creators use their contracts and acceptable use policies to set out clearly the limits of what the customer is allowed to do with the AI product or service they deploy (see for example Salesforce’s Acceptable Use Policy). We support the Commission’s suggestion that citizens should be clearly informed when they are interacting with an AI system and not a human being.
- Robustness and accuracy of AI systems: In the B2B context, as discussed above, AI creators develop tools that can be used by many customers. Customers have varying degrees of control over which data is used to train models, which data is predicted against, and what predictions are made, all of which can be changed at any time. Robustness and accuracy are very use-case specific, and the most AI creators can do is make tools for their customers to measure robustness and accuracy.
- Human oversight: This is without doubt an important element, however, it can be undermined, e.g. if the human involved is not incentivised to ensure the system is making the most accurate/safest decision, or if the human is not given enough information to validate the AI decision/recommendation. Therefore it is important that the right incentives are in place. For instance, in Salesforce’s Acceptable Use Policy it is clearly stipulated that our customers may not use our general-purpose AI products as part of a decision-making process with legal or similarly significant effects, unless the customer ensures that the final decision is made by a human being. In this case, the customer must take account of other factors beyond the Salesforce services’s recommendations in making the final decision.
- Clear safety and liability rules: Clarity on the safety and liability regime that is applicable to AI applications is welcome. In that context, we would like to note that in the B2B environment, rights and obligations of the parties, including on liability, are thoroughly negotiated and clearly stipulated in the contract between the two parties. Contractual freedom gives also the opportunity to the two parties to tailor liability considerations to the specific context of the use of AI which, as demonstrated earlier, is of the utmost importance for assessing risk. As discussed above, it is important to keep in mind that AI creators often create general tools, and it is up to the customer how these tools are

employed. Similar to the GDPR, the company with the means to control the means and purpose of the AI tool's use should be directly liable to the affected individuals.

- Compliance and Enforcement:
  - For high-risk applications, we would support a combination of ex-ante self-assessment of compliance and ex-post enforcement. If the Commission opts for the ex-ante assessment of compliance by means of an external conformity assessment procedure, it should ensure that the conformity assessment body will have the necessary resources, including the right in-depth expertise and adequate staff, to perform these assessments effectively. There should also be a careful consideration of the impact that a rigorous ex-ante compliance check would have on the development and deployment of innovative AI solutions. For instance, it could significantly slow down AI adoption in Europe (considering also the possible scenario where an AI application does not squarely fit into the "high-risk" definition, in which case its developers or users are likely to take the prudent approach and wait for the positive assessment before putting the AI in question on the market or deploying it). Additionally, the mere volume of new applications being put in the market could quickly overwhelm the conformity assessment body, creating a large backlog of assessments and approvals.

Comments on "Safety and liability implications of AI, IoT and robotics"

- Overall, we would welcome more clarity on the liability regime that is currently applicable to AI applications. However, as with risk, liability should be considered in a context-specific manner.
- AI can take many forms and be used in a variety of ways. In the great majority of cases, the existing safety and liability regime is sufficient. We would encourage the Commission to undertake a thorough exercise of identifying the gaps in current legislation as well as the specific AI use cases where the gaps might appear. Focusing on specific sectors, rather than on the risk from which AI users should be protected, could inadvertently limit innovation in these areas, while failing to address real concerns.
- If the Commission were to proceed with introducing new liability rules for AI systems, these should be limited to high-risk applications. In the case of low-risk applications, the existing safety and liability regime is sufficient.
- The Commission is right to recognize in the White Paper that "each obligation should be addressed to the actor(s) who is (are) best placed to address any potential risks".
- Looking specifically at the B2B context in which Salesforce operates, the rights and obligations of the parties, including on liability, are thoroughly negotiated and clearly stipulated in contracts. Contractual arrangements give also the opportunity to the two parties to tailor liability considerations to the specific context of the use of AI, which is also of the utmost importance for assessing risk. We can draw a useful comparison with the concepts of data controller and data processor, as these are described in the GDPR. In B2B, the controller (ie the user of AI) should be the one liable to consumers, while processor liability should be via contract with the controller. Even fully automated systems often depend on the data submitted, and how the predictions are then used, both of which are in the hands of the controller. B2B processor liability should be when the AI tool doesn't perform as specified, and just like in the GDPR, any potential future liability regime for AI could make sure that the contract between B2B processor and controller has certain terms in place.

Thank you for the opportunity to provide comment to this important initiative. We remain at your disposal, should you require further information.