Brussels, October 14, 2025

# Re: Call for Evidence – Simplification – digital package and omnibus

Salesforce welcomes the opportunity to provide comments to the European Commission's call for evidence on the Digital Omnibus (Digital Package on Simplification).

The European Union's ambition to become a global digital leader is being challenged by its own fragmented and complex regulatory framework. Despite having strong research and innovation capabilities, the EU has struggled to turn these into a competitive advantage, especially in advanced technologies like artificial intelligence (AI). To unlock its full potential and complete its Digital Single Market, Europe needs a simpler, more coherent, and consistent legislative framework for digital policies.

## The Imperative for Simplification and Coherence

A fragmented legal and regulatory landscape across the 27 EU Member States creates a patchwork of rules that confuses businesses, increases compliance costs, and slows down the development and deployment of digital services. A 2024 report by the European University Institute's Centre for a Digital Society stated that "the number of new laws that have been introduced to promote digitalisation (...) is simply enormous"[1]. "The future of European competitiveness" Report by Professor Mario Draghi calls for a 25% cut in overall reporting obligations[2] and it highlights the importance that a more joined-up approach to policy coordination across all EU institutions can play to foster growth and competitiveness.

Fragmentation is particularly harmful for Europe's numerous startups and SMEs, which are often the main drivers of innovation but lack the resources to navigate a complex legal

[1] p.11 MARCUS, J. Scott, ROSSI, Maria Alessandra, Strengthening EU digital competitiveness : stoking the engine, EUI, RSC, Research Project Report, 2024, Centre for a Digital Society - https://hdl.handle.net/1814/76877

[2] p. 69 The future of European competitiveness report, by Professor Mario Draghi, https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en#paragraph_47059

415 Mission Street
San Francisco,
California 94105
Salesforce, Inc.
/salesforce
@salesforce

environment. The lack of a true Digital Single Market means that a company developing a new service or technology must often adapt it to different national laws, leading to significant delays and higher costs. This discourages investment and makes it harder for European companies to scale up and compete with global players. The issue is not the sheer number of laws, but also their overlaps and inconsistencies, which risk stifling innovation and preventing firms from scaling and competing internationally.

## Boosting AI with Harmonized Rules

The European Commission has made it clear that they want to boost AI development in the EU. As Commission President Ursula von der Leyen has stated, "This is the mission of the next decade to make Europe one of the leading AI continents".[3] However, without a streamlined legal framework, this ambition is at risk.

The effectiveness of the EU AI Act hinges on clarifying and proportionally applying its substantive requirements. Its foundational risk-based approach is undermined by overly broad designations (e.g., in Annex III), which risk inadvertently over-regulating low-risk systems, creating significant legal uncertainty and hindering the consistent implementation across all Member States. This issue is compounded by the persistent fragmentation of the EU's wider digital policy on data governance and cybersecurity, which can create contradictory requirements that stifle innovation. For instance, a lack of consistent rules on data access and use across different sectors could severely limit the data available for training robust AI models. The Draghi report made this point clearly, stating that "regulatory barriers to scaling up are particularly onerous in the tech sector, especially for young companies". It also warns that the EU's "regulatory stance towards tech companies hampers innovation".[4]

To address this, the EU must move toward a more coherent, technology-neutral approach. Regulatory frameworks need to be agile and forward-looking to adapt to the latest technological developments, such as generative AI and agentic AI. Simplifying the regulatory framework would provide the legal certainty that companies need to confidently invest in and deploy AI solutions. This would benefit private enterprise, public administrations, and critical sectors like manufacturing and healthcare, ultimately enhancing Europe's competitiveness.

---

[3] Opening keynote speech by President von der Leyen at the 'One Year After the Draghi Report' Conference, September 16, 2025
https://ec.europa.eu/commission/presscorner/detail/en/speech_25_2102
[4] p. 32 The future of European competitiveness report, by Professor Mario Draghi,
https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en#paragraph_47059

# Data Protection as an Enabler, Not a Barrier

Crucially, this push for simplification does not mean compromising the fundamental protection of Europeans' personal data. The EU's commitment to data privacy, as enshrined in the GDPR, is not under question. The goal is for data protection principles to coexist with and enable innovation, not hinder it. Consistency of laws and regulations can in fact strengthen data protection by bringing clarity and coherence on core principles.

The GDPR and the EU AI Act should work in tandem. The EU AI Act provides a legal framework for the safe development of AI systems, while the GDPR ensures the protection of personal data used by those systems. Data protection should be viewed as a way to build trust with citizens and provide legal certainty for businesses, thereby fostering innovation rather than stifling it. By focusing on clear, consistent implementation and providing practical guidance for how GDPR principles apply to new technologies, the EU can ensure that it remains a global leader in both innovation and data governance.

A good practical example of AI in the service of privacy are AI agents. With the right guardrails, AI agents can fortify a company's privacy efforts, minimizing human error, limiting data access by design, and acting as privacy intermediaries. Agentforce, the agentic layer of the Salesforce Platform, empowers businesses to configure agents with strict boundaries when processing personal data, prioritize data minimization, and ensure compliance with global privacy regulations. For example, an AI agent can be configured to present an organization's privacy statement to individuals at the first point of contact, provide "just-in-time" notices if at any point further personal data is collected from individuals, and provide up-to-date and relevant information on how to exercise data subject rights on request. Agents could also be configured to help consumers better understand a company's privacy policies by creating a conversational interface for them to ask questions, demystifying complex legal jargon, and fostering transparency.

In this paper, we present our concrete and targeted suggestions including (i) clarifications to the EU AI Act to strengthen legal certainty and alignment with existing EU rules; (ii) improvements to the GDPR to strike the right balance between robust data protection and the development of AI; (iii) improvements to other data-related regulations; and (iv) the streamlining of cybersecurity requirements.

415 Mission Street
San Francisco,
California 94105
Salesforce, Inc.
/salesforce
@salesforce

# Our proposals

## Proposals for the EU AI Act

### Designation of “high-risk” in the EU AI Act

- **The issue:** High-risk designations in the EU AI Act should be more narrowly tailored to capture truly high-risk activities. For instance, according to Annex III (4), AI systems in the areas of “employment, workers management and access to self-employment” are high-risk. However, such a broad reference may capture use cases that should not be considered high-risk. AI has been used for administrative tasks in recruitment for years, such as for resume matching and filtering. AI can help recruiters and employers to match opportunities to those workers that are genuinely qualified or interested. As long as a human is in the loop for the ultimate hiring or dismissal decisions, these use cases should not be *de facto* considered high risk. The stated goal of the EU AI Act is to “guarantee safety, fundamental rights and human-centric AI, and strengthen uptake, investment and innovation in AI across the EU”[5]. This goal and the Act’s risk-based approach will be better served from clear and narrow interpretations of high-risk, which in the example presented above, would mean limiting the high-risk designation to AI systems that are used without human intervention or review.
- **Our proposal:**
    - Avoiding overly broad designations will enhance legal certainty and boost the uptake of these innovative solutions by European industry. We have presented our detailed position on this matter in our response to the European Commission’s public consultation on the classification of AI systems as high-risk. As a first step, we believe that the upcoming guidance is an excellent opportunity for the European Commission to provide the necessary clarity on this issue.
    - While we understand that exceptions are contemplated in the derogations from the high-risk classification requirements in Article 6(3), the steps to establish a derogation to the high-risk designation are burdensome (e.g. documentation and registration). Therefore, we would encourage the Commission to provide clarification by narrowing the designation rather than requiring such exceptions to follow the derogation requirements.
    - Therefore, as part of the Digital Omnibus or the upcoming Digital Fitness Check, we urge the European Commission to consider modifications to Annex III (4), as

[5] European Commission website on the AI Act: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

415 Mission Street
San Francisco,
California 94105
Salesforce, Inc.
/salesforce
@salesforce

well as similar review and simplification of all Annex III use cases. Additionally, we suggest amending Article 6(3) as follows: “By derogation from paragraph 2, an AI system referred to in Annex III shall not be considered to be high-risk where it does not pose a significant risk of harm to the health, safety or fundamental rights of natural persons, including by not materially influencing the outcome of decision-making or by ensuring meaningful human intervention or review”.

### Aligning obligations of high-risk AI providers with other EU legislative frameworks

- **The issue:** Certain requirements of a high-risk provider under the EU AI Act may be read to contradict provider obligations as a data processor under the GDPR. For example, post-market monitoring requirements under the EU AI Act seem at odds with a processor's obligation to only process data for very limited purposes as dictated by customer instructions (e.g. related to providing the service).
- **Our proposal:**
    - We recommend revisiting these obligations, in particular limiting the requirement on providers to an obligation to provide deployers with the tools required to conduct the post-market monitoring themselves.
    - Alternatively, we recommend clarifying that the provider's post-market monitoring obligations are solely with regard to system-level risks, and do not require access to the deployer's environment.
    - We also recommend ensuring incident response requirements in the EU AI Act align with incident response requirements in other regulations (e.g. GDPR) rather than conflict and/or create net new requirements. This will prevent the creation of redundant, conflicting, and resource-intensive reporting obligations, thereby allowing resources to be focused on actual security and safety.

### Streamlining enforcement

- **The issue:** The enforcement of the EU AI Act involves a combination of centralized and decentralized structures, with national market surveillance authorities, the European Commission (via the AI Office), and the European Data Protection Board all playing roles in the enforcement process. The number of players involved in enforcement will inevitably result in inconsistencies.
- **Our proposal:** We invite the European Commission to consider the introduction of a mutual recognition framework to address the risk of fragmentation and inconsistency in the EU AI Act's enforcement. A mutual recognition framework will foster consistency across national authorities, meaningfully advancing the goal of a single, harmonized EU

415 Mission Street
San Francisco,
California 94105
Salesforce, Inc.
/salesforce
@salesforce

market for AI. The principle of mutual recognition dictates that a product (in this case, an AI system) lawfully placed on the market or certified as compliant in one Member State should be automatically accepted as compliant by all other Member States. A mutual recognition framework would require a national authority to accept the conformity assessment or the compliance certification issued by another Member State's Notified Body or authority. This would eliminate the ability of one national authority to reject an AI system that has already been approved elsewhere, and advance consistent interpretation of the AI Act's horizontal rules.

### Mutual recognition of existing international standards

- **The issue:** The European Commission is facing delays in developing the technical standards for the EU AI Act, which are essential for turning the law's principles into concrete rules. Companies are left with uncertainty on how to achieve compliance, making it difficult to prepare for the law's upcoming deadlines. This uncertainty not only stifles innovation but also puts a strain on companies, particularly SMEs, who can't afford to risk non-compliance.
- **Our proposal:** To address this, the European Commission should prioritize the mutual recognition of internationally recognized standards, such as ISO 42001. This approach would allow companies to use globally accepted benchmarks to demonstrate compliance, rather than waiting for EU-specific standards that may be years away. By recognizing existing international standards, the EU would provide immediate clarity and a practical pathway to compliance for businesses worldwide. This would also ensure consistency, as companies in different member states could all rely on the same well-established standards. This framework would accelerate the adoption of safe and trustworthy AI while maintaining the EU's goal of a harmonized market.

## Proposals for the intersection of Data Protection and AI

### Aligning Data Subject Rights to AI needs

- **The issue:** The GDPR's Data Subject Rights in Articles 15 (access), 17 (erasure), and 21(objection) create significant challenges for the development and deployment of AI models. Once data has been used to train an AI model, it becomes inextricably embedded within the model’s learned parameters. “Model unlearning” can be technically challenging or require disproportionately costly retraining of the entire model, effectively demanding the destruction of a valuable asset built on significant investment.

415 Mission Street
San Francisco,
California 94105
Salesforce, Inc.
/salesforce
@salesforce

- **Our proposal:**
    - We encourage the European Commission to acknowledge that the rights to data access and erasure present unique challenges when personal data has been processed for the purpose of training an AI model, where such data becomes deeply and inseparably embedded within the model's architecture. In such cases, and where the controller has taken all reasonable technical and organizational measures, including data minimization, anonymisation and pseudonymization prior to training, to prevent the retention of personal data within the model's parameters, the right to access, erasure, or objection shall not be interpreted as requiring the complete retraining, deletion or expungement from the AI model. The controller shall, however, provide the data subject with an explanation of how their data is being used and the practical limitations of its erasure from the model itself.
    - Where complete erasure, access, or objection is not technically possible without disproportionate impact on model integrity, public interest, or the rights and freedoms of others, alternative measures may be implemented, including:
        - Certification of data minimization, anonymization, or pseudonymization prior to training;
        - Model training documentation;
        - Provision of high-level summaries of model logic or decision criteria;
        - Use of synthetic data to mitigate personal data dependency.
    - These recommendations do not waive the fundamental rights of data subjects, but guide proportionate enforcement in AI-specific contexts.

### Re-imagining the legal basis for training

- **The issue:**
    - Consent is a challenging legal basis to use in practice when training AI models, leaving companies with fewer options and often forcing them to rely on legitimate interest (LI), which requires a Legitimate Interest Assessment (LIA). The issue is that the data used for AI training may not have been collected under circumstances that meet LI requirements.
    - This creates legal uncertainty for companies developing AI. We believe the concept of consent needs to be fundamentally revisited to make it a more workable legal basis for AI development. The European Commission should also provide clearer guidance on how to use LI for AI development.
    - This is precisely what the CNIL, the French data protection authority, did with its guidance from June 2025, which supports using LI as a legal basis for AI training, provided certain conditions are met. By promoting LI through practical, detailed

415 Mission Street
San Francisco,
California 94105
Salesforce, Inc.
/salesforce
@salesforce

guidance, the CNIL offers a model for a more flexible and realistic approach to data governance for AI development, giving companies much-needed legal clarity.

- **Our proposal:**
    - We recommend that the CNIL approach is promoted among regulatory and enforcement authorities as helpful guidance regarding the use of LI as a legal basis for processing personal data, particularly in the context of AI system development and training. This guidance can serve as a practical and immediate approach for organizations navigating the complexities of data protection in AI.
    - In the longer term, we propose clarifying Recital 32 in the GDPR as follows: "When personal data is processed for the development of artificial intelligence systems, particularly for the purpose of training an artificial intelligence system or model, consent should cover all processing activities carried out for that development purpose, provided that the data subject is informed in a clear, concise, and non-disruptive manner about the nature of the AI system being developed and its intended functionalities. To ensure that the purpose limitation principle is applied to future applications of the artificial intelligence system or model, the type of system or model being developed should be described along with an illustration of its key potential functionalities, thereby fulfilling the requirement for a specific, informed, and unambiguous indication of agreement.**"**

## Streamlining Data Protection Impact Assessments (DPIA), Records of Processing Activities (ROPA), Legitimate Interest Assessments (LIA), Transfer Impact Assessments (TIA)

- **The issue:** The current compliance structure for data protection particularly as it applies to AI companies operating globally, is not streamlined for efficiency but rather based on separate, overlapping documentation requirements, involving separate, repetitive DPIAs, TIAs, ROPAs, and LIAs. This creates an excessively burdensome and highly costly compliance environment that promotes non-compliance over genuine risk mitigation.
- **Our proposal:**
    - To resolve this complexity and foster a pragmatic and proportionate regulatory environment, we propose to consolidate DPIAs, TIAs, and LIAs into a single, tiered Integrated Risk Assessment document.
    - Separately, the requirement for *every single exporter* to independently evaluate the laws of non-adequate third countries is repetitive and costly. We urge the European Commission to publish Regional Risk Profiles for non-adequate countries, which companies can rely on for the foreign law analysis and only

415 Mission Street
San Francisco,
California 94105
Salesforce, Inc.
/salesforce
@salesforce

perform a supplementary check on residual risks specific to their processing activity.

### Data anonymization

- **The issue:** The GDPR's high bar for true anonymization is compounded by the capabilities of modern AI. The European Data Protection Board requires that anonymization be assessed case-by-case, requiring that the risk of re-identification be sufficiently remote based on all means reasonably likely to be used. Because true anonymization is virtually impossible to prove, data intended for AI analysis is often regulated as personal data even if minimal risk exists. This risks unnecessarily triggering the full compliance regime (DPIAs, consent, rights of erasure) for low-risk applications.
- **Our proposal:** We encourage the European Commission to develop a more realistic and achievable technical threshold for how difficult it should be to re-identify or reverse anonymized data, specifically for non-sensitive or low-risk data. This would set a clear, risk-based benchmark, thus preventing the stifling of beneficial data use and analysis across the vast majority of less sensitive applications. It would also strengthen data protection, as currently, many companies don't take actions that would meaningfully protect data, because they fall short of the existing standard for anonymization.

## Proposals on data-related regulations

### GDPR: Cross-border data transfers and data "in the clear":

- **The issue:** The "no data in the clear" standard for cross-border data transfers, stemming from post-*Schrems II* guidance from the European Data Protection Board[6], is unclear and often a friction point. It is not aligned to the operational reality of modern, global cloud SaaS services, which require some level of data processing in clear (decrypted) form to function.
- **Our proposal:** We call the European Commission to initiate a targeted consultation with regulators, industry, and other relevant stakeholders, to develop risk-based, proportionate guidance that distinguishes between data processing "in the clear"

[6] EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data https://www.edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en

415 Mission Street
San Francisco,
California 94105
Salesforce, Inc.
/salesforce
@salesforce

necessary for the core functionality of a standard SaaS contract, and the unnecessary or high-risk exposure of sensitive data.

### GDPR: Addressing the weaponization of DSARs in employment disputes

- **The issue:** The use of Data Subject Access Requests (DSARs) as a "weapon" in employment disputes is escalating across the EU, forcing employers into disproportionate data disclosure efforts and risking the privacy rights of colleagues and third parties named in communications.
- **Our proposal:** Following the UK's recent, more nuanced guidance on addressing "manifestly unfounded or excessive" requests, which offers a clearer path to challenge DSARs made with a malicious or harassing intent, we propose that the European Commission issue clarification or guidance on Article 12(5) and Article 15(4) of the GDPR. This must explicitly empower data controllers to refuse or strictly limit the scope of DSARs in employment contexts where the primary motive is demonstrably vexatious, purely for litigation discovery, or when responding fully would necessitate the disclosure of third-party personal data that cannot be reasonably redacted or anonymised without disproportionate effort or prejudice to those individuals' rights.

### EU Data Act

- **The issue:** Chapter VI of the Data Act contains obligations for providers of data processing services to facilitate and enable customers' switching to other services. To comply with these requirements, Salesforce has updated its online services terms with a dedicated Data Act Addendum to address customer needs. We believe that more targeted guidance and additional clarifications are needed to ensure effective data portability and interoperability.
- **Our proposal**: We call the European Commission to swiftly adopt targeted non-binding guidelines aimed at identifying the current interoperability obstacles, allowing B2B providers to make available to their customers self-automated tools able to easily initiate and complete the switching process. We believe that allowing standards and other industry initiatives to evolve will reduce costs and speed up the switching process for European companies.

415 Mission Street
San Francisco,
California 94105
Salesforce, Inc.
/salesforce
@salesforce

# Proposals on cyber-related regulations

## Streamline Incident Reporting Requirements

- **The issue:** Managing cyber incident response and recovery is challenging enough without the added complexity of multiple reporting frameworks. GDPR, NIS2, DORA, and CRA regulations each have their own specific criteria and scope for incident reporting. This can create a significant burden, forcing organizations to report the same incidents multiple times and in different formats, each with unique technical and language requirements. For entities like Salesforce operating across multiple jurisdictions, this duplication increases operational costs and complexity without improving response effectiveness.
- **Our proposal:** We invite the European Commission to further exchange with Member States in order to establish a single, national-level entry point for all relevant reports. Additionally, an alternative solution could be the creation of a single reporting platform within the European Union Agency for Cybersecurity (ENISA). This could serve as a powerful tool to route reports to the appropriate national authorities. It would maintain the integrity of national entry points while creating a resilient, efficient system that avoids a single point of failure.

## Align “Main Establishment” Definition

- **The issue:** The current EU cybersecurity landscape, with regulations like CRA, DORA and NIS2, often presents a challenge for companies. The use of different terminology to define similar concepts such as “main establishment” creates confusion and makes compliance complex, especially for businesses operating across multiple frameworks. This complexity can lead to a misallocation of resources, as organizations are forced to prioritize compliance over proactive mitigation, response, and recovery efforts. This ultimately weakens the EU's overall cyber resilience and diminishes the benefits of centralized reporting offered by ‘main establishment’ concepts as a whole.
- **Our proposal:**
    - We recommend the European Commission to leverage the upcoming CSA review to ensure that the definition of “main establishment” is aligned across multiple frameworks, including the CRA, NIS2 and the GDPR, using the definition provided in NIS2 as the common reference point. This would allow entities falling under the scope of more than one framework to rely on a harmonized and legally consistent definition and interpretation of their main establishment for reporting purposes.

415 Mission Street
San Francisco,
California 94105
Salesforce, Inc.
/salesforce
@salesforce

- Additionally, to ensure consistent application and interpretation of NIS2 across all 27 Member States, we recommend the European Commission issue clear guidance on the legislative intent behind the "main establishment" concept. This will promote the uniform application of the law and protect the ultimate goal laying behind the One-Stop-Shop mechanism: strengthening EU's cyber resilience.

415 Mission Street
San Francisco,
California 94105
Salesforce, Inc.
/salesforce
@salesforce