Non-paper on reducing the regulatory burden of the digital rulebook

The Netherlands welcomes a concerted effort to reduce unnecessary and disproportionate regulatory burdens of the digital rulebook for public and private entities, while at the same time preserving the digital rulebook's overarching objectives. We must ensure the digital rulebook is implemented such as to enable innovation and growth and bolster legal certainty and protection. The digital rulebook strengthens the internal market and thereby makes the whole Union more resilient. The Netherlands believes the digital omnibus and complementary initiatives to reduce the regulatory burden of the digital rulebook should be developed in consultation with a broad group of stakeholders according to three principles:

1. The goals of adopted digital legislation must stay intact. An omnibus must focus on clarification, increasing consistency and complementarity. The cumulative effects of the legislation should be assessed to identify opportunities for better alignment or increased coherence.

2. Reduce cost and efforts for compliance, especially for governments and SMEs by providing practical tools and assistance:
   - Guidelines, formats, model contracts and standards that ease the burden of compliance should be provided swiftly;
   - Definitions, reporting formats and tools should be streamlined and consolidated where possible.
   - A centralised European reference guide could help organisations navigate the regulatory landscape and its definitions.

3. Streamlined and consistent governance is instrumental. The European boards created for the governance of the digital rulebook should have a large role in consistent application and interpretation of law and policy. Currently, the boards vary in their effectiveness and insufficiently facilitate consistency across regulation.

The Netherlands looks forward to working with the EU institutions and member states to reduce the administrative burden in the digital domain. We believe the following actions should be considered to reduce the regulatory burden of the digital rulebook.

AI

- Prioritise simplification of implementation. Clarity about what is needed to comply with the AI Act is of utmost importance to improve trust and establish a European internal market for human-centric and trustworthy AI. Therefore, providing more clarity is a preferred strategy above extending deadlines.
- Define critical infrastructure. We encourage the Commission to draft a common list of infrastructure considered critical under Annex III, point 2. It is currently unclear which infrastructure is considered critical. This risks fragmentated interpretations at a national level and higher compliance costs due to uncertainty.
- Create clarity, but leave room for flexibility. The Commission should continue drafting templates (such as those on role allocation or risk classification) and other tools to support the compliance efforts of providers and deployers. However, providers should have flexibility to adapt certain procedures to their specific circumstances, as long as this does not create conflict with the goals of the AI Act. An example is to create a possibility to deviate from the template of the post-market monitoring plan of article 72(3).
- Extend the derogation for Quality Management Systems (QMS) of article 63(1) to SMEs. The QMS and post-market monitoring are expensive aspects of the compliance activities.

Cybersecurity

- Investigate streamlining cybersecurity legislation. An impact assessment for streamlining cybersecurity legislation should be fast-tracked. The impact assessment should identify which proposed solutions will effectively reduce regulatory burdens, while taking into account the increase in workload caused by changes made while legislation is still being implemented.
- Identify the advantages and challenges of a Single Reporting Platform (SRP) before introducing this idea in new legislation. It is currently unclear whether a SRP on an EU and national level will

effectively reduce the regulatory burdens for incident reporting. A SRP should demonstrably contribute to reducing the regulatory burden.
- Streamline reporting obligations where feasible. Some reporting obligations (such as from NIS2 and CER) can easily be merged due to their similar nature. We see practical and legal challenges for reporting obligations where reporting frequency, purpose, mandate and responsibilities vary profoundly (such as from CRA and GDPR).

Data

- Strengthen the European Data Innovation Board (EDIB). The EDIB should be provided with sufficient financial and administrative support to exercise its tasks as set out in the Data Act and Data Governance Act (DGA). The governance for data legislation should be streamlined to avoid overlapping or redundant governance structures.
- Clarity on international non-personal data flows. A single, coherent regime on international data flows should be created. The relation between the provisions on international data flows in article 31 of the DGA, article 33 of the Data Act and the GDPR are insufficiently clear. The GDPR's adequacy decisions framework offers a strong foundation to build upon. Providing similar clarity for non-personal data can decrease the administrative burden.
- Allow data intermediaries to develop revenue streams. The provisions for data intermediation services, such as those in article 12 of the DGA, should be amended to strengthen the economic viability of European data sharing initiatives.

Data Protection

- Provide practical tools to make compliance easier for smaller organisations. We encourage supervisory authorities to continue developing practical tools, such as templates and model clauses. Specifically, lists of low-risk processing activities provided by supervisory authorities can provide clarity. Such guidance could be made the norm or even mandatory, by amending article 35(5) of the GDPR.
- Explore how the development and use of codes of conduct can be increased. Codes of conduct can be useful tools to facilitate compliance. However, they are rarely developed. The reasons for this are not entirely clear. We propose to explore how the development and use of codes of conduct can be stimulated, for example by simplification of the approval process.

Electronic Privacy

We observe practical challenges both for enterprises seeking to comply with ePrivacy legislation and for users experiencing consent fatigue being confronted with repeated consent requests.

- Explore exemptions for cookies or similar technologies for purely analytical purposes. Any exemption should be without prejudice to the GDPR.
- Protect the fundamental rights and freedoms of users, empowering them to make effective choices regarding cookies, fingerprinting and other technologies. This can be achieved through technical solutions such as user-controlled browser settings, in line with GDPR consent requirements. Such solutions would drastically reduce the regulatory burden of compliant consent flows, while having a meaningful impact on reducing consent fatigue.