DIGITAL SERVICES ACT (DSA)

IBM'S POSITION PAPER

MARCH 2021

IBM a multinational technology company serving clients in over 170 countries. With more than 100 years of commitment in Europe, IBM is one of the largest technology employers in the EU and has many cloud data centers, research labs, innovation spaces, centers of excellence, etc. spread across Europe. IBM scientists from 50+ nationalities work in Europe on cutting-edge research and IBM will build Europe's first quantum computer in Germany.

IBM's expertise is in the intersection of technology and business, providing artificial intelligence (AI) and cloud-based solutions that are changing the way the world works. Above all, guided by principles for trust and transparency and support for a more inclusive society, IBM is committed to being a responsible technology innovator and a force for good in the world. For more information, visit www.ibm.com.

INTRODUCTION

As a global Business-to-Business (B2B) technology company with a significant European footprint, IBM plays a key role in the digital transformation of Europe's industry, enabling our clients to benefit from the power of data. Cloud technologies, AI, Blockchain, IoT, and data analytics will continue to be crucial to increase the resilience of key sectors in Europe's economies and build technological sovereignty.

With greater digitization comes greater responsibility: IBM believes that the safety of users online is paramount and we have earned the trust of our clients by responsibly managing their most valuable data, committing to our Trust and Transparency principles, ensuring that we can protect client data and insights, and preventing illegal content from spreading across the Internet.

Digital services providers should be responsible for the societal impact of their platforms: this has become an even greater imperative at a time when the use of digital technologies has accelerated amidst the ongoing COVID-19 crisis and will be an essential part in the recovery of our society and economy.

Therefore, **IBM welcomes the European Commission's proposal for a Digital Services Act (DSA).** We are pleased the Commission adopted a "*precision regulation*" approach that is focused clearly on placing more responsibility on the relevant platforms to tackle illegal content online, something IBM has long called for.

We believe this proposal is an important starting point to build greater trust in technology and can offer an opportunity for Europe to champion online responsibility and accountability, while allowing digital businesses to continue to grow and innovate.

IBM'S COMMENTS ON THE DIGITAL SERVICES ACT

1. Maintaining a differentiated scope and limited liability for hosting services:

Companies providing online services to individuals and whose content is being disseminated to the public should be responsible for the societal effects those services can have, including facilitating criminal and terrorist activity and impacts on children and on elections: therefore, we **fully support the Commission's targeted approach, creating a new "online platform" category and requiring different rules for different categories of services:**

- The term "digital services" broadly encompasses today a large number of companies, business models, or services, many of whom play little to no role in the proliferation of illegal content online. For example, the business model of "pure" B2B services providers set them apart from the large platforms operating in the

consumer space. They deliver services designed to increase the efficiency and agility of businesses and processes of their enterprise clients, They do not offer content sharing services for end-consumers or the general public, and therefore do not have the ability to control, edit or curate user-generated content that may appear online.

- This is why **passive intermediaries such as mere conduit, caching or passive hosting services, particularly B2B services, should continue to benefit from intermediary liability exemptions, and should not be subject to the same enhanced content moderation obligations as online platforms and very large online platforms (VLOPs).**

- **We support maintaining such differentiation in the scope of the DSA, consistent with recent EU legislation such as the Terrorist Content Online Regulation**: a one-size-fits-all approach that would impose the same rules on all digital services would create disproportionate burden for many businesses particularly in the B2B sector. Such an approach would limit the uptake of cloud and emerging technologies across businesses, particularly SMEs. This could limit innovation in the EU and damage the broader data economy, as well as Europe's technological sovereignty.

2. Focus on illegal content:

We also support the Commission's approach and believe that regulatory efforts should focus on acting against illegal content (Article 8). Indeed, we believe that harmful content should be tackled separately, such as through voluntary or co-regulatory approaches.

In practice, IBM reserves the right to take measures against customers whose activities might not be illegal but may cause harm: our cloud services agreement[1] sets out various restrictions on how our services may be used:

"*Cloud Services may not be used for unlawful, harmful, obscene, offensive, or fraudulent Content or activity. Examples of prohibited activities are advocating or causing harm, interfering with or violating the integrity or security of a network or system, evading filters, sending unsolicited, abusive, or deceptive messages, introducing viruses or harmful code, or violating third party rights".*

This broad language gives us the flexibility, in appropriate circumstances, to request our clients, if we believe they have violated the terms of our agreement, to remove legal, yet harmful, content. We also reserve the right to suspend/terminate the services if the client fails to remove such content.

[1] *https://www.ibm.com/support/customer/csol/contractexplorer/cloud/csa/be-en/11*

3. *No general monitoring obligation:*

We support the prohibition of a monitoring obligation (Article 7). This is particularly important for B2B service providers (e.g. Cloud service providers) like IBM, who generally have no contractual rights and no technical access to content that enterprise customers store or process on our services. Only the enterprise customers have absolute control and responsibility over their own content and the services they operate.

General monitoring of cloud content would be a complex undertaking, requiring us to re-engineer our service offering, and would also pose significant privacy issues should we be required to monitor personal, financial and medical data of potentially millions of data subjects, as well as the content of corporations and governments. Such a monitoring obligation would disincentivize business customers from moving to the cloud.

4. *Know your Business Customer (KYBC):*

We support the Commission's approach, limiting KYBC obligations to online platforms that allow consumers to conclude distant contracts with traders (Article 22).

We would specifically caution policymakers against expanding the proposed scope of these KYBC provisions and requiring that such obligations should be horizontally implemented by all digital services beyond online platforms: the objective of KYBC obligations is first and foremost to ensure consumers are protected against dishonest businesses selling illegal products online, therefore such rules should first take into account the role of digital services that are an active party in the provision of a B2C goods or services.

However, the provision of core services to regulated sectors such as operators of essential services depends entirely on the ability to provide robust cloud solutions that are neither designed nor intended to/directed at consumers. Many times, enterprise cloud-based solutions are offered on a "Pay as You Go" principle, which has contributed to the success of the cloud, particularly among small businesses and developers, hence the need to safeguard the smoothness and speed of online business operations.

Many B2B cloud services already implement strong safeguards to prevent fraudulent businesses from using our cloud services (e.g., contractual obligations in our service contracts, security-based services against fraud). Additional and disproportionate KYBC requirements may not only raise privacy and/or business confidentiality concerns, but could discourage companies, particularly SMEs and start-ups, from moving to the cloud, if held up from accessing services pending clearance.

SPECIFIC ISSUES IN CONTENT MODERATION RELATING TO B2B CLOUD SERVICES AS THEY ARE PROVIDED TO BUSINESS CLIENTS

Client data and the insights produced on IBM's Cloud or from IBM's AI are owned by IBM's clients. This is a core feature of our business model. As a provider of B2B cloud services, this is an essential difference between business models and services like ours, and consumer-oriented services such as social media platforms; video streaming services; or video, image, audio or file sharing services.

Because our clients' data belong to our clients, **we cannot remove specific content on our customers' websites, do not deploy any tools to monitor our clients' content and do not have the ability to identify illegal content ourselves**. Only our business customers have absolute control and responsibility over their own content and the services they operate.

Our limitations to tackle illegal content are both technical and contractual:

- **Technical:** IBM does not have control over its clients' data. Additionally, clients may, and often do, choose to encrypt their data on our cloud infrastructure. We give our clients the ability to keep the encryption key and we do not have any access for security and privacy reasons.

- **Contractual:** our cloud services agreement[2] limits the potential scope of IBM's access to, or use of, the client's content. In practice, this is a very limited right to access, and we do not have the right to monitor or modify the content:
  - *"Content Content consists of all data, software, and information that Client or its authorized users provides, authorizes access to, or inputs to IBM Cloud Services.*
  - *Client grants the rights and permissions to IBM, its affiliates, and contractors of either, to use, provide, store, and otherwise process Content solely for the purpose of providing the IBM Cloud Services.*
  - *Use of the IBM Cloud Services will not affect Client's ownership or license rights in Content.*
  - *IBM, its affiliates, and contractors of either, will access and use the Content solely for the purpose of providing and managing the IBM Cloud Service.*
  - *IBM will treat Content as confidential by only disclosing to IBM employees and contractors to the extent necessary to provide the IBM Cloud Services."*

  Altering contracts to allow IBM access to content for monitoring purposes would be very likely to discourage businesses from moving to the cloud for security and privacy reasons.

[2] *https://www.ibm.com/support/customer/csol/contractexplorer/cloud/csa/be-en/11*

As a responsible technology company, we do, however, have "notice and action" processes in place to tackle illegal usage of our services (as outlined in our **Acceptable Use Policy**[3]), which are as follows:

- If we are made aware of the presence of illegal content on a client website, our abuse department will first assess the validity of the complaint from the content that is on the public website (NB: as IBM does not have any control over its business customers' data, it can only "see" what is visible on the public Internet and can only identify and inform the customer with whom IBM has a contractual relationship, who may be the party responsible for managing this content).

- If the complaint is deemed valid, IBM will notify our customer asking the content to be removed expeditiously (or ask our customer to instruct their customer to remove it). If the customer fails to remove the content or to have it removed by the person/entity who uploaded it, according to the notified timeframe, IBM will suspend the service or block access to the server for that particular customer (NB: as IBM does not have the ability to remove the specific content directly, the only option is to shut down the server in its entirety).

Regarding the nature of the content itself, the vast majority of the complaints we receive involve content infringes a trademark or copyright (IP) of a third party. Most of the time (well over 90%) the actual publisher of the infringing content is not a direct customer of ours, but rather a customer of one of our customers.

***

[3] *https://www.ibm.com/services/us/imc/html/aup1.html*