



Public Consultation on Regulation of cloud computing services

December 2024

I. Introduction

Cloudflare welcomes the opportunity to submit our views to ARCEP in response to its recently published consultation. We highlight the importance of ensuring the competitiveness of cloud services across the French economy, as well as the potential for these services to drive better security and efficiency outcomes. We believe that ARCEP can help set the expectations and guidelines that will ensure businesses benefit from the transition to the cloud at minimal cost.

In this submission we respond to ARCEP's questions on the effect of excessive data migration costs on our customers' ability to take full advantage of multi-cloud and multi-vendor architectures.

We do not address the full list of consultation questions in this submission, however, we do put forward our primary concerns and possible solutions. We would also acknowledge our previous conversations and submission to ARCEP regarding this topic and address some of the points raised below.

II. Background: Cloudflare's Connectivity Cloud

We would first like to give an overview of Cloudflare's position within the overall cloud market as well as how we, through our business model and practices, encourage pro-competitive behavior for the benefit of our customers and the ecosystem.

The world has moved away from legacy IT systems, which were traditionally made up of hardware run on premises and licensed software stored on the local hardware, and towards cloud-based technologies that eliminate the cost and complexity of managing and integrating hardware. As they make this transition, however, organizations want the ability to use a variety of different systems, from those that remain on premises, to those on the Internet and in public clouds, to software as a service (SAAS) and other products and services.

When it comes to accessing cloud services, our customers want to connect remote teams, local teams and infrastructure, multiple cloud environments, SaaS apps, and more, so that they function like a single, secure environment. This means that products must be easily interoperable, without any additional costs from data transfer, so that users are able to select the best provider for their needs. Customers want to be able to easily move their data and connections to other providers to suit those needs and as new options emerge.

Cloudflare believes that businesses should be able to choose the best cloud services for their needs. That means that businesses and consumers should be empowered to evaluate offerings and should not face artificial barriers to using services from a range of providers. Cloudflare's

[connectivity cloud](#) enables our customers to connect any services, public clouds or on premises resources they have, giving them the ability to share information, connect their data in a fully interoperable way providing both security and performance at the same time.

By its nature, this is a pro-competitive approach and an antithesis to the way the dominant cloud providers have traditionally run their businesses, which is based on vendor lock-in and uncompetitive bundling practices and with the ultimate aim of driving up prices.

Within this context, we have welcomed the recently adopted EU data regulation (“Data Act”) and in particular its ban of switching fees which came into force on 11 January 2024. We argue in this submission, however, that the implementation of these changes needs to go further in order to achieve maximum benefit for both cloud services and their customers. We highlight the continued distorting practices of high data transfer costs as well as certain interoperability issues, which our customers have raised with us as challenges to cloud switching and multi-cloud setups.

III. The impact of recent data regulation on egress fees

A number of large cloud providers, namely AWS, Microsoft and Google have, announced a programme of providing free egress following the adoption of the EU Data Act. Google, for example, [announced](#) that it will remove data transfer fees for customers moving off Google Cloud. As confirmed in its announcement, “the cost for customers to migrate data out of a cloud provider is minimal”. On 5 March, AWS then also [announced](#) the removal of data transfer fees for customers moving out of AWS, and finally, on 13 March Microsoft made a similar [announcement](#).

While these changes by the hyperscalers may be a move in the right direction, we would caution against concluding that it solves vendor lock-in due to the high costs associated with egress fees. Because the EU Data Act intends to eliminate egress fees for multi-cloud architectures in addition to the removal of fees when switching providers, we would stress that the hyperscalers’ announcements have not gone far enough.

We would like to point to a number of concerns:

- The change implemented by the hyperscalers [does not waive](#) egress fees by default: customers need to specifically apply for free data transfer and obtain the hyperscalers’ agreement.
- Waiving egress fees is only available to those customers who are moving ALL of their data out of the hyperscalers’ cloud and are ending their entire relationship with the hyperscaler in question and its services.
- Customers moving only a portion of their data, who are not completely migrating off the hyperscalers’ cloud, are not required to terminate their agreement with the hyperscaler and will still pay egress fees. In Google’s words: “Data transfer charges remain for normal customer activities. The data transfer credits are only for customers who are leaving Google Cloud.”

Hyperscalers are therefore only eliminating a small part of the egress fees they were levying before. Customers wanting to move only part of their data, because they want to obtain a specific service from another provider (such as Cloudflare) while leaving a portion of their data on the hyperscalers' cloud, will still have to pay egress fees, even when the hyperscalers incur no cost from the data transfer. This does not help customers looking for a specific best-in-class service elsewhere, nor those looking to implement a multi-cloud strategy for their business.

It is important to note that egress fees are applied by hyperscalers to all data taken out of a cloud, not just data taken out to switch to another provider. In fact, any time a customer's data leaves a cloud provider - for instance when someone downloads content from a website or application or transfers data for analysis through software stored in a different cloud provider - egress fees are levied. In other words, every time a customer imports data from a cloud provider to an application stored on another cloud provider, they incur egress fees. Notwithstanding the hyperscalers' announcements referenced above, egress fees therefore continue to serve as a disincentive for customers to leave a cloud provider's ecosystem.

While this change in practices around egress fees may be the hyperscalers' answer to the provisions in the EU Data Act, it does little to enhance fair competition and does not ultimately help those smaller and most innovative players in the market, who are the most disadvantaged.

European AI startups, for example, can use Cloudflare's storage capabilities to store large amounts of unstructured data, used for training AI models, without incurring costly egress fees associated with typical cloud providers. In Cloudflare's experience, there is a disproportionate impact on SMEs who wish to store their data using a multi-cloud solution, and we would therefore encourage ARCEP to ensure the hyperscalers go further in their efforts to eliminate these costs.

IV. The varying costs of data transfer

We welcome ARCEP's approach to the application of the EU Data Act, which was implemented into French law in May 2024¹. Article 27 of the new law adequately reflects the freedom of choice for cloud service users by capping data transfer and provider switching fees. For these laws to be applied with the intended effect, we agree with ARCEP that a more granular approach of looking at the different ways in which cloud providers leverage data costs is needed. This needs to go beyond only prohibiting suppliers from charging data transfer fees over a maximum amount (*yet to be defined by ARCEP*) in the context of switching.

Although we do not comment on all the questions laid out in the consultation paper, we do recognise that egress fees are not solely limited to those incurred when switching cloud providers. We also address the different costs associated when data is migrated from one cloud provider to another as well as the discounting of data transfer fees which extends every time traffic is delivered from the cloud.

¹ Law No. 2024-449 aimed at securing and regulating the digital space, SREN law

a) The costs associated with the transfer of data related to infrastructure

The data transfer fees charged by many cloud providers can be an integral part of the cloud hosting bill. Since cloud providers use their own global telecommunication backbone or use transit service providers to carry traffic, they may incur infrastructure costs that get passed on as data transfer fees to their customers. However, these data transfer fees are typically charged regardless of whether cloud providers incur infrastructure costs as part of the data transfer. As noted in the consultation document, the cost of transmitting data depends on how the data is transmitted. There are broadly three ways in which networks interconnect to exchange data:

1. **Private Network Interface (PNI):** This is where networks connect directly – literally a cable between the routers of networks as a “neutral” “carrier hotel” data center. For PNI, there are small setup costs and a small charge from the carrier hotel for the wire that connects the networks. These costs are generally thought of as negligible.
2. **Internet Exchange Peering:** When two networks are both members of the same Internet Exchange, traffic can be exchanged there. Internet exchanges are many-to-many. Any network that is present at the exchange can exchange traffic with any other member. This is a low-cost method of exchanging data between networks.
3. **IP transit:** The last option, where neither of the first two are available, is to send data from one network to another via a 3rd party IP transit network. For IP transit, one (usually smaller) network pays another (usually larger) network to carry its traffic to the rest of the Internet. Generally IP transit networks are paid based on the 95th percentile (near the peak) of the data that is sent through them over the course of a month.

For nearly all major cloud providers, traffic that is delivered to Cloudflare users passes across a private network interface (PNI) or private interconnection. As outlined above, this is dedicated capacity leased from the owner of fiber optic cables that we can use to connect two locations. Unlike when there's a transit provider in between, there's no middleman, so the cloud provider bears no incremental costs for transferring the data over this PNI. For example, for transferring log files from our edge servers, Cloudflare may choose to use backbone capacity to send data from its location in Vienna to its processing location in Amsterdam, instead of sending that data on a transit network. This keeps the costs low and the network running efficiently.

b) The costs associated with transit

In most instances, Cloudflare exchanges traffic without the use of transit providers. Cloudflare peers with more than 13,000 networks globally, and is present in more than 250 public Internet Exchange Points worldwide. Cloudflare has an open peering policy and will peer with networks that have a presence on mutual exchange points. As with most exchanged traffic, the overwhelming majority of Cloudflare's traffic is exchanged on settlement free terms.

For traffic that is transmitted through transit providers, generally, transit fees are charged at a unit rate based on the 95th percentile of traffic that flows between the networks, subject to a minimum commitment. For example: assume we have 10 total ports with a transit network in 10 different cities, and each port has 100 Gigabits of capacity. Our total capacity with the transit

provider is 1.000 Gigabits (1 Terabit). In a given month, the 95th percentile might be 600 Gigabits per second across all the ports. Assuming that traffic is above the commitment we made, we would be charged our unit rate multiplied by the traffic (per Mbps).

For reference, [Telegeography](#) has stated they see market transit rates of ~\$0.12 / Mbps in Europe, and see these continuing to slowly decline. Big networks will get better pricing than the market average in recognition of the higher volumes of traffic. In our example, 600 Gbps (600,000 Megabits per second) * \$0.10 per Mbps = \$60,000 monthly charge.

As described above, these fees do not apply when data is exchanged via private peering or data exchanged at an Internet exchange, which is the case for the vast majority of transfers.

Cloudflare's costs for transferring data out of our network, for example, vary widely depending on where the data is going. For data sent to a network with which we have settlement-free peering (which we do with most cloud providers), our costs are negligible. This is important because the nature of this network is that data comes to us in the closest possible way. This keeps costs low, an advantage that is passed onto customers. This also underlines the importance of free and open peering between different networks. In fact, free and open peering benefits not just Cloudflare's network, but also the networks of the large cloud providers, in turn keeping their costs low as well.

c) Additional costs incurred for cloud providers

For Cloudflare to directly connect with 13.000 networks, it uses multiple 'points-of-presence' (PoPs). This interconnection is done through a mix of carrier-neutral PoPs and embedded caches within the networks of Internet Service Providers (ISPs). The vast majority of Cloudflare's PoPs are in rented spaces for servers in data centers, in addition to these PoPs within ISP networks.

The cost of adding a PoP within an ISP's network is smaller than at a carrier-neutral site. In addition, some PoPs are more critical than others. While the cost of adding a PoP within an ISP network can be hundreds of thousands USD, adding a tier-1 PoP to our network will cost a multiple of that (given these need to offer significant capacity, i.e. consist of many more servers, as well as incur recurring fees for other resources).

Setting up a new PoP may include the cost of hardware (servers, routers, cables, as well as the cost of importing this equipment into the jurisdiction), the rent of data center housing, the cost of ensuring resilient connectivity (usually through transit providers) and engineering staff time. However, once set up, the cost of running the additional PoP consists chiefly in the ongoing fees for connectivity and the fees for renting space.

In addition to the elements related to PoPs above, Cloudflare's network includes a '[backbone](#)', consisting of rented capacity on a number of long-distance fiber optic cables. This backbone, offered in an integrated way within our services, allows our customers to benefit from faster traffic when needed. Cloudflare's software continuously calculates the most efficient routes for our customers' data based on our global network. This software turns the existing networks that

constitute the Internet, including the legacy slow-performing ones, into the smart, fast and reliable Cloudflare network that our customers need.

V. Cloudflare has limited visibility into the degree of switching costs

Although Cloudflare provides a variety of network services to customers we do not generally monitor the traffic flows of our millions of customers. Our customers determine how to configure our services and have opportunities to monitor their traffic flows themselves, which means that we have limited visibility into the total costs incurred for customers looking to switch providers. It is also important to stress that it is not always our customers who initiate a given data transfer: it could simply be someone accessing their website or application. In that scenario as well, data may egress from the cloud provider the customer uses. In most cases, therefore, the main additional costs associated with migration between services or switching from one cloud provider to another, lie entirely within the customer's environment and are difficult to predict. Although some transfers of data may involve additional transit costs, too often, we see cloud providers charging for egress of data even when direct interconnection means there is no substantive cost for that transfer.

This makes it impossible for us to respond to questions related to the costs incurred which exist solely in the customer environment.

VI. Conclusion

Although we recognise that there can be different costs associated with the transfer of data, there are many cost-negligible ways for a customer to port data from one cloud provider to another. Cloud providers should be encouraged to minimize their own costs and pass those savings on to their customers, rather than charging for costs in order to lock in their customers. We also appreciate that certain costs related to infrastructure set up and transit could be costly to certain cloud providers, however these have not historically been commensurate with the costs passed on to customers and should be kept to a minimum. In most instances, therefore, we maintain that the cost of data egress should not exceed the cost of ingress.

We welcome the opportunity to discuss any points above with you further should this be helpful.