Regeringskansliet
Justitiedepartementet
103 30 Stockholm
Sweden

Dnr: Ju2017/07896/Å

Sent by email to Ju.a@regeringskansliet.se and by mail.

BCC Comments on Proposed Data Retention Regulation in Sweden

We are grateful for the opportunity to comment on the proposals for data retention regulation set out in the report[1] ("the Heuman Report") by the Swedish government rapporteur, Sigurd Heuman, Chairman of the Security and Privacy Protection Board.

The Business Carrier Coalition ("BCC") is an industry coalition which represents the interests of a number of international telecommunications providers comprised of AT&T, BT, Colt Technology Services, Orange Business and Verizon Enterprise Solutions. The BCC provides a vehicle for issues of common interest to its members to be raised and presented to relevant regulatory stakeholders across Europe, the Middle-East and Africa.

The BCC members provide predominantly large international business users, in both the private and public sectors, with advanced electronic communications services across Sweden, the European Union (EU) and the rest of the world. None of the BCC members provide services to consumers in Sweden.

BCC members take regulatory compliance very seriously and information security is at the heart of our businesses. Indeed security is paramount for BCC members given the complex international environment we operate in and the type of customers we typically serve. This has led BCC members to develop best-in-class security practices with strict and extensive policies that are fully enforced across our respective companies in the EU and globally.

As described more fully below, we first provide our view on the compatibility of the proposal with EU Law. Then we reiterate our overall position with regards to data retention in general and more specifically raise our concerns with the proposed requirements for retained data to be stored in Sweden, and for NAT addresses. The localisation requirements are a key concern to us and we do not believe that such requirements are proportionate or justified.

[1] SOU 2017:75 Heuman Report, including English Summary, available at: http://www.regeringen.se/4a8d12/contentassets/b635202b96fc4e4490886e0ef8601e66/datalagring--brottsbekampning-och-integritet-sou-201775

The compatibility of the proposal with EU law

The judgment in Tele2 / Watson[2] and the earlier judgement by the CJEU reflects continuity in the Court taking a strong stance on data protection and privacy. While the Court acknowledged that fight against serious crime may depend on modern investigative techniques, this cannot in itself justify general and indiscriminate data retention. In fact the Court stated that such legislation should be restricted to what is strictly necessary and that such retention should be evidence based and should objectively make it possible to "identify a public whose data is likely to reveal a link, at least an indirect one, with serious criminal offences".[3] The proposal as it stands does not meet this criteria and others set out by the CJEU. Therefore, BCC members believe there is a high risk that the proposed legislation would yet again be in breach of EU law.

BCC position on Data Retention

Although we fully recognize the necessity for law enforcement measures in this area, we believe they can be disproportionate in the case of high end business providers such as the BCC members. As opposed to the consumer space, our services are characterized by low volumes of high-end business users that rely on internal systems of control against non-appropriate use of electronic communications services. As a result we only receive a very low volume of requests from LEAs[4] for data retained in line with our legal obligations. With this in mind it is worth noting that a number of EU countries have taken a more targeted approach to the scope of their approaches.

In Finland, data retention obligations only apply to companies specifically designated by the home ministry.[5] In return, the government is responsible for the costs of systems and software acquired for the support of the authorities that benefit from the data retention.[6] The Finnish system has the advantage that it creates incentives for authorities to only impose data retention obligations on companies where such an obligation is proportionate to the desired outcomes and provides a necessary safeguard against abuse.

The UK has implemented a similar approach whereby the obligation to retain data applies only to communications providers that have been served a retention notice[7] by the Home Office. Such providers are then able to recover a contribution towards their costs to ensure that they can establish, operate and maintain effective, efficient and secure infrastructure and processes to meet their obligations. We regret that the previous and proposed continued system in Sweden is disproportionate and burdensome particularly for players that rarely get such requests if at all.

BCC members have serious concerns about the proposed requirement for retained data to be stored in Sweden

The Heuman Report claims that retained data should be stored in Sweden for reasons of "crucial state interests" and "national security":

---

[2] Joined Cases C‑ 203/15 and C‑ 698/15,
[3] See Judgment in joined Cases C‑ 203/15 and C‑ 698/15, p. 103 – 111
[4] Law Enforcement Agencies
[5] Finnish Information Society Code Section 19 157 §
[6] Finnish Information Society Code Section 37 299 §
[7] UK Investigatory Powers Act 2016, Section 87

> **"Protection and security levels, retention in Sweden and destruction**
> The data subject to the retention obligation should not be allowed to be stored outside Sweden. The CJEU states only that national legislation must prescribe that electronic data storage may not take place outside the EU. However, confining the retention to Sweden would enable more effective supervision while improving protection of both individuals' confidentiality and national security. Since the matter now in question concerns crucial state interests, there are no EU legal barriers to prescribing that storage takes place only in Sweden."[8]

BCC members are providers of cross border business services: our operations are, by nature EU wide and international. Following the CJEU ruling on the EU DR Directive, BCC members not only now face a confusing patchwork across the EU (status quo, annulment of legislation or new rules emerging), but also new obligations to require providers to store data in-country (so-called data localisation).

BCC members believe that imposing such localisation requirements in Sweden would impose unnecessary and disproportionate costs on their operations in terms of acquiring, operating and staffing storage facilities in Sweden. We do not believe that such a requirement is justified as illustrated by existing EU centralized storage solutions (where retained data from several EU countries are stored in a single location) that continue to provide highly secure data storage in full compliance with specific national requirements (e.g., data categories to retained, retention periods, etc.) and, significantly, without any impairment to the ability of authorized authorities to have prompt access to the data and that both under the EU Directive and following the ECJ ruling. Localisation requirements in Sweden would not de facto provide Swedish citizens with any greater guarantee over the confidentiality of their data, nor would it provide authorized Swedish authorities with more effective access to the retained data. On the contrary, we would argue that centralized storage offers a more effective and secure solution for the international business providers, such as BCC members, than spreading resources thinly across the EU to meet multiple local storage mandates in the event that several other countries were to follow the proposed Swedish example.

For the most part, the categories of data to be retained under the new proposal mirror closely the data BCC members already retain for commercial and billing purposes. The "e-Privacy" Directive[9] established the principle of the free movement of personal data within the EU. This means that the same data for which Sweden is contemplating an in-country storage mandate is already stored in other parts of the EU in compliance with existing rules. Creating a duplicative storage obligation for Sweden LEA purposes would therefore be disproportionately costly. More importantly, this illustrates that the data as such is not labelled as national security data in the day to day operational context.

BCC members also wish to highlight that several reports concluded that it was not necessary for retained data to be stored in Sweden, nor indeed, elsewhere within the EU, to guarantee access to

[8] Id. at page 44.
[9] Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector

data by competent Swedish authorities.[10] This included the 2015 Heckscher report[11] for the Swedish government on data storage integrity that argued that if there is no genuine national security justification for mandatory storage in Sweden, the proposed requirement is contrary to the basic principles of EU law, since it essentially hinders the freedom of establishment (Articles 49-54 Treaty of Functioning of the European Union - TFEU), the free provision of services (Articles 56-52 TFEU) and the free flow of personal data between Member States as provided for in both the General Data Protection Regulation[12] and the "e-Privacy" Directive. More importantly as also recognised by the European Data Protection Supervisor (EDPS): "Physical location is not the determining factor in security"[13]. BCC members are concerned at the prospect of significant compliance costs to meet an in-country storage mandate which would be wasted if the requirement is eventually appealed and annulled (as happened in the case of previous data retention legislation). The proposal would mean that the BCC members would have to make large additional investments on top of the investment already made in our centralized data retention solution.

In addition, unless the Swedish government intends to fully meet operators' capital and operating costs of implementing in-country data retention storage capabilities, any "per request" compensation mechanism will not be of any assistance to BCC members where we have already implemented data retention laws in compliance with national laws across the EU (including Sweden's earlier annulled requirements) and we have never received any requests or warrants for any retained data.[14]

Translation of NAT addresses

We also wish to take the opportunity to highlight our concern with the requirement that would oblige operators to translate addresses where Network Address Translation (NAT) is used.

This requirement is unprecedented, as typically only data processed by operators for operational purposes are required to be retained. The obligation to translate addresses behind a NAT poses multiple technical challenges. In most cases, NAT is performed on customer premises and therefore the IP address information is not available to the operator. In other situations, NAT is performed at various points in the network (e.g., ingress and egress points of the network) where the operator

---

[10] "Our assessment is therefore that control by an independent authority is guaranteed in Swedish law even with regard to suppliers that might choose to store data outside the EU. Moreover, we have found that a requirement in national law for retention within the EU or the EEA is incompatible with other EU regulations in the area and with Sweden's commitments under the Data Protection Convention. Against this backdrop, our assessment is that no general prohibition should be introduced against data that is retained under Swedish data retention rules being transferred to a third country for storage there." *Data Storage and Integrity* ("Heckscher Report"), English Summary available at: http://www.regeringen.se/49bb84/contentassets/116590d7d8824b458b4142fe9f3624f5/datalagring-och-integritet-sou-201531 (page 26)

[11] SOU 2015:31

[12] Regulation (EU) 2016/679

[13] https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2015/15-04-28_Keynote_Cybsersecurity_EN.pdf (page 6)

[14] See these examples of transparency reports of BCC members:
AT&T: http://about.att.com/content/dam/csr/Transparency%20Reports/Aug-2017-TransparencyReport.pdf
Verizon: http://www.verizon.com/about/portal/transparency-report/international-report/

cannot technically collect the required IP information without significantly re-architecting and reconfiguring its network. This obligation would require the design of an entirely new retention system, imposing considerable costs on the operator to solution and maintain. BCC members regard this new obligation as disproportionately burdensome, especially in light of the likely absence of any warrants or requests.

Conclusion

In conclusion, we urge the Swedish authorities not to adopt the Heuman report proposal for retained data to be stored in Sweden, or, at the very least, identify a means of exempting international business service providers from any data localization mandate in line with the proportionality argument. Given the additional costs it would entail we also request that the requirement on translation of NAT addresses be deleted.

Please do not hesitate to contact us should you require further information on this issue.

Respectfully submitted this 29 of January 2018 by the BCC – Business Carrier Coalition

For more information, please contact:

- For AT&T: Dominique Baroux at +33 1 4188 4538 or baroux@att.com
- For BT: Emanuele Vadilonga at +44 207 356 6044 or emanuele.vadilonga@bt.com
- For Colt Technology Services: Ulf Wahllöf at +46 (0) 8 781 80 60 or Ulf.Wahllof@colt.net
- For Orange Business: Isabelle Dieltiens at +32 2 643 94 72 or isabelle.dieltiens@orange.com
- For Verizon : Åke Florestedt at +46 (0) 8 5661 7522 or ake.florestedt@se.verizon.com