



Dear Secretary-General Jagland,

We the undersigned organizations write to you today in support of the 28 June 2018 [submission](#) “Joint Civil Society Response to Discussion Guide on Protocol to the Convention on Cybercrime”, and as a follow-up to our [3 April 2018 statement](#), which requested more civil society input to the drafting of the Convention’s second additional protocol.

We join our colleagues who wrote the June joint [submission](#) in expressing our concern that the Convention’s second protocol could inadvertently serve as a vehicle for bypassing human rights standards for the collection, handling and retention of personal data. Improperly crafted, we believe the second protocol could enable rights-damaging forum shopping by some law enforcement, and a race to the bottom for protection that trends towards the data handling protections of states with the worst privacy standards for all the Convention’s signatories. If drafters are fully cognizant of this risk and the consultation process is rigorous, we are confident that such pitfalls can be avoided.

As we’ve mentioned previously, Convention 185 of the Council of Europe (the “Cybercrime Convention”) has had remarkable reach in terms of signatories – having been ratified not only by a large number of CoE Member States, but also by large and small states from around the globe. As a result, we see the Cybercrime Convention’s second additional protocol as critically important both for its direct impact on the data handling practices of the many European and non-European state signatories, and for the strong example it sets for non-signatory states – for good or potentially for ill.

It is crucial that the Cybercrime Convention avoid the mistakes of examples like the U.S. CLOUD Act, or the European Commission’s own proposals for transborder data, access, which omit critical human rights safeguards, and in particular in the case of the EU proposals, they inappropriately burden service providers with judging the appropriateness of law enforcement requests for themselves, with too many incentives to over-comply, without due process. .

We therefore request your close attention to the key recommendations and concerns raised by our colleagues’ joint submission. In particular, we wish to highlight:

1. The submission’s recommendation that the convention’s deliberations prioritize refinement of the Mutual Legal Assistance Treaties (MLAT) system for bilaterally handling cross-border data requests, rather than creating a compromised universal standard for convention signatories;
2. The necessity of “dual data privacy protection”, according to which requests for data must be legal by national laws in both the requesting and receiving country;
3. That a narrow and time-bound definition of any ‘emergency’ standards that may be adopted is critical. We would emphasize the recommendation to limit this to direct and immediate threat of serious harm to life, rather than much lower thresholds such as potential harm or the protection of state interests;
4. That states that are party to Convention 185 should also sign, ratify and properly implement Convention 108+, which provides for comprehensive and detailed data protection in the use and transfer of data that Convention 185 does not;
5. That extremely robust transparency and accountability mechanisms must be built into the final agreement, with yearly public reporting and as much transparency to those whose data is shared as possible.



The global network  
DEFENDING AND PROMOTING  
FREE EXPRESSION

With best regards,

ARTICLE 19

Afghanistan Journalists Center (AFJC)  
Africa Freedom of Information Centre (AFIC)  
Americans for Democracy & Human Rights in Bahrain (ADHRB)  
Association for Technology and Internet (APTI) - Romania  
Bits of Freedom  
Bytes for All (B4A)  
Cartoonists Rights Network International (CRNI)  
Child Rights International Network (CRIN)  
Digital Rights Ireland  
Digital Rights Watch  
Electronic Privacy Information Center (EPIC)  
Epicenter.works  
Eticas Foundation  
Frënn vun der Ënn  
Hermes Center for Transparency and Digital Human rights  
Hiperderecho  
IT-Political Association of Denmark  
Pacific Islands News Association (PINA)  
Privacy and Access Council of Canada  
Privacy International  
Rocky Mountain Civil Liberties Association  
SHARE Foundation (Serbia)  
Usarios Digitales  
Vrijschrift (The Netherlands)  
X-Net