To: Alexander Seger, Head of the Cybercrime Unit of the Council of Europe

CC: Ms Dunja Mijatović, Council of Europe Commissioner for Human Right
Mr Thomas Schneider, Chair of the Steering Committee on Media and Information Society (CDMSI)
Mr Patrick Penninckx, Head of the Information Society Department at the Council of Europe
Ms Sophie Kwasny, Head of the Data Protection Unit of the Council of Europe

20.11.2019

Dear Mr Seger,

We, the undersigned organisations, believe that enabling effective police investigations is important but that, at the same time, requests for personal data across borders must comply

with human rights protections. The procedures proposed by the Cybercrime Convention Committee (T-CY) exacerbate the challenges of the Cybercrime Convention (CCC), and create the potential for serious interference with human rights.

You will find attached a consultation response on the T-CY Committee's Second Additional Draft Protocol, prepared by EFF, EDRi, IT-Pol Denmark and EPIC. We urge the Council of Europe and its Parties to take these comments fully into account.

Notably, we encourage the Cybercrime Committee of the Council of Europe to consider the following recommendations. We believe that the Draft Protocol:

- Should not include new mechanisms for compelled subscriber information production without the involvement of Parties on both sides;
- Should clarify the scope of section 4 to exclude data from individuals' ongoing use of a service that allows precise conclusions concerning the private lives and daily habits of the individuals concerned. It should also clearly ensure that section 4 should be applied to subscriber data as defined in CCC, excluding logon information, dynamic IP addresses, and location data, as well as records of carrier-grade NAT (CGN) IP address and port number mappings;
- Should exclude dynamic IP addresses, log-on IP addresses as examples of subscriber information;
- Should exclude location data or any data that can reveal precise conclusions concerning the private lives and daily habits of a subscriber such as records of carrier-grade NAT (CGN) IP addresses and port number mappings;
- Should require Parties to ensure that data disclosed pursuant to it will not, cross-referenced with other data, result in an unexpected level of intrusion on individuals' private lives;
- Should include a dual criminality requirement for the issuing of an order;
- Should require prior judicial authorisation by a court or an independent judicial authority to issue an order in all instances;
- Should reiterate the need for Parties to comply with Article 15 of the CCC, Conditions, and Safeguards and with international human rights law; Due process and legal safeguards should be respected before disclosing the identity of anonymous speakers online.
- Should require member countries to first sign and ratify Convention 108+ for the protection of individuals with regard to the processing of personal data;
- Should make the notification to the requested Party, including the possibility to halt the direct disclosure of data, mandatory for all Parties;
- Should only impose a gag order after a careful independent authorisation by a court;
- Should impose a minimum factual predicate necessary to indicate that the person investigated is believed to be planning, committing, or has already planned or committed criminal acts;

- Should adopt security measures such as encryption and authentication mechanisms for the delivery of requests and responses;
- Should ensure that the Parties' domestic laws do not impose undue restrictions on freedom of expression;
- Should ensure that the Requesting Parties publish, at a minimum, aggregate information on the specific number of cross-border orders approved and rejected as well as a disaggregation of the requests by service provider and by investigation authority, type, and purpose, and the specific number of individuals affected by each;
- Should provide service providers all the information needed to review each order and the possibility to oppose it as appropriate.

We still believe that the priority of the T-CY Committee should be to improve Mutual Legal Assistance Treaties and increase their efficiency.

We look forward to cooperating with the Council of Europe in order to improve future mechanisms for cross-border access to data in line with human rights standards.

Yours sincerely,

Electronic Frontier Foundation (EFF) – International
European Digital Rights (EDRi)

Access Now
Alternative Informatics Association Turkey
Article 19
Australian Privacy Foundation (APF)
Canadian Access and Privacy Association (CAPA)
Canadian Institute of Access and Privacy Professional (CIAPP)
Derechos Digitales - Chile
Digital Rights Foundation (DRF)
Državljan D – Slovenia
East European Development Institute - Ukraine
Electronic Privacy Information Center (EPIC) – United States
Fundación Datos Protegidos - Chile
Hiperderecho – Peru
Homo Digitalis - Greece
Huaira Foundation Quito - Ecuador
IPANDETEC - Central America
IT-Pol Denmark
#SeguridadDigital - Mexico
Tedic - Paraguay