The Right to Privacy in Denmark
Stakeholder Report, Universal Periodic Review, 24th Session

Privacy International (PI) and IT-Political Association of Denmark (IT-Pol) submitted a stakeholder report to bring their concerns about the protection and promotion of the right to privacy in Denmark before the Human Rights Council for consideration in Denmark's upcoming Universal Periodic Review in early 2016.

The following key issues were raised along with relevant recommendations and questions:

Review of anti-terrorism legislation
In the first cycle UPR review of Denmark, the issue of privacy was raised by stakeholders. In the Working Group report, the Netherlands recommended that Denmark "carry out an inclusive evidence-based evaluation of the Danish anti-terrorism legislation". Denmark did not accept this recommendation, but merely noted it. Currently, Denmark is adopting new anti-terrorism laws with more surveillance powers (including collection of passenger name records, PNR) in response to the attacks in Paris and Copenhagen in early 2015.
We recommend the Government of Denmark to:

- *Ensure that all anti-terrorism measures, including those currently being proposed or being adopted, adhere to international human rights law and standards and respect the right to privacy;*
- *Initiate an independent evidence-based evaluation and open consultation of the anti-terrorism legislation, so that the necessity and proportionality of the current legislation can be properly assessed before new legislation is introduced.*

Question: Would the Government of Denmark consider carrying out an evidence-based evaluation of the Danish anti-terrorism legislation, and opening up the drafting process allowing for a public consultation?

Data retention
In April 2014, the Court of Justice of the European Union (CJEU) ruled that the Data Retention Directive was in violation of the Charter of Fundamental Rights of the European Union. The directive mandated the retention of telecommunication data about the entire population without any link, even an indirect or remote one, with serious crime. The Government of Denmark maintains that the national data retention law, which also covers the entire population, is not in violation of the Charter. On a positive note, in June 2014, the Danish Minister of Justice repealed the session logging provisions, which mandated retention of source and destination IP addresses as well as port numbers for all internet packets. However, according to news media report in January 2015, the Ministry of Justice is considering to re-introduce session logging.

We recommend the Government of Denmark to:

- *Ensure that a proper evaluation of the Danish data retention law is made in the current parliamentary year, including a full review of its compliance with the Charter of Fundamental Rights and the CJEU data retention judgment, and Denmark's other international human rights obligations;*
- *Not to re-introduce session logging which is very intrusive on citizens' right to privacy as full details of their internet activities are stored.*

Question: Would the Government of Denmark consider reviewing the data retention legislation in order to ensure compliance with the right to privacy and other fundamental rights?

Interception of communication

Subject to a court order, the Danish police can intercept telephone calls and internet communication. Furthermore, the special data reading provision allows the police to access non-publicly available information in a computer system using trojan software or other equipment. This practice amounts to computer network exploitation (CNE), commonly known as hacking, which is an extremely intrusive form of surveillance. This provision is particularly concerning as it does not provide for any restriction on the type of information, there is very little publicly available information about the use of this power, and there has been little public or Parliamentary oversight.

We recommend the Government of Denmark to:

- *Ensure that all communication surveillance laws, including data reading, adhere to international human rights law and standards and respect the right to privacy.*

Question: Would the Government of Denmark be willing to review the data reading (state hacking) provisions to comply with international human rights law?

Surveillance by the Danish foreign intelligence service

The Danish Defence Intelligence Services (DDIS) can collect any type of information as long as the operation is directed against conditions abroad. Raw data from mass surveillance of electronic communications can be shared with other intelligence services without any legal restrictions. The only safeguard is that DDIS cannot process information about Danish citizens unless this is done by coincidence. A new law, currently being adopted, will allow targeted collection against Danish citizens abroad in terrorism cases. The suspicion standards are lower than in ordinary Danish criminal law. Oversight of DDIS is limited, and only Danish citizens have access to redress with the oversight board if they believe information about them is processed unlawfully.

We recommend the Government of Denmark to:

- *Ensure that intelligence sharing arrangements with foreign partners are in accordance with international human rights law and provide to Danish citizens a clear understanding of the legal nature of the relationships;*
- *Recognise that the right to privacy applies to all citizens and take steps to reduce the discrimination against foreign citizens in the DDIS law.*

Questions:

1. What steps will the Government of Denmark take to increase the effective oversight of DDIS, especially in connection with the new targeted surveillance of Danish citizens abroad?
2. What measures will the Government of Denmark take to protect the right to privacy for foreign citizens in connection with the operations of DDIS?