DECLARATION OF IT-POLITICAL ASSOCIATION OF DENMARK
UPR PRE-SESSION ON DENMARK, GEVEVA, 17 DECEMBER 2015

Presentation of the organisation

This statement is delivered on behalf of IT-Political Association of Denmark. IT-Political Association of Denmark is a digital rights organisation that works to promote privacy and freedom in the information society. We are regularly consulted by Danish news media and politicians in privacy and surveillance matters.

National consultations for the drafting of the national report

For the national consultations, the Danish Ministry for Foreign Affairs held four meetings for the general public in February 2015, each of which addressed a specific human rights issue. In September 2015 there was a public consultation (in writing) on the draft national report.

Plan of the Statement

This statement is based on our UPR stakeholder submission together with Privacy International. The statement will address the following issues

1. The Danish anti-terrorism legislation
2. Telecommunication data retention
3. Mass surveillance by defence intelligence agencies

Statement

1. The Danish anti-terrorism legislation

A. Follow-up to the first UPR review
In the first UPR review, 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. In the mid-term review in 2014, the Government's response for this recommendation was changed to ”under consideration”. This was a positive development.

The Government appointed an evaluation committee which began its work in early 2015. However, after the election in June 2015, and a change of government, the Ministry of Justice decided to terminate the work of the committee in October, and no evaluation report was produced.

B. New developments since the first review
After the terrorist attacks in Paris and Copenhagen in early 2015, the Government proposed new

anti-terrorism measures in February 2015. This is the third anti-terror package since 2001.

The new measures include social media monitoring and establishment of a national system for passenger name records (PNR) where all data will be directly accessible by Danish intelligence services.

Furthermore, the Danish Defence Intelligence Service (DDIS) will get new powers for targeted surveillance of Danish citizens abroad in terrorism cases. Although this will be subject to a court order, the suspicion standards are lower than in criminal law.

It is very concerning that new anti-terror legislation is proposed by the Government without an independent review of the effects of the existing legislation, which include measures as intrusive as computer network exploitation (CNE), that is state hacking, in the special "data reading" provision adopted in 2002.

C. Recommendations
We call upon the Government of Denmark to:

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

2. Telecommunication data retention

A. Follow-up to the first UPR review
There were no recommendations on this issue.

B. New developments since the first review
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. Information about telephone calls and location data from mobile phones are still retained for 12 months. With the increasing use of smartphones that constantly generate internet traffic, this means that an almost complete location history is stored for most citizens.

On a positive note, in June 2014, the Danish Minister of Justice repealed the special session logging provisions in the data retention law, which effectively required the retention of a complete history of all websites visited for the past 12 months.

The official reason for the repeal of session logging was that it had been unable to achieve its stated objective, not the CJEU data retention judgment. The Ministry of Justice reserved the right to re-introduce session logging, and according to news media report, this is already under consideration.

C. Recommendations
We call upon 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;
- Not to re-introduce session logging which is very intrusive on citizens' right to privacy as full details of their internet activity are stored.

3. Mass surveillance by defence intelligence agencies

A. Follow-up to the first UPR review
There were no recommendations on this issue.

B. New developments since the first review
Following the revelations of Edward Snowden in 2013, there has been increased public attention to the interception of electronic communication by defence intelligence agencies around the world.

The Government of Denmark has refused to recognise the mass surveillance documented by the Snowden revelations as a threat to the privacy of Danish citizens and even refused to investigate specific cases of alleged foreign spying in Denmark.

The Danish Defence Intelligence Service (DDIS) under the Ministry of Defence has wide-ranging powers to intercept electronic communication as long as the operation is directed against conditions abroad.

Information about Danish citizens may be collected as ”raw data” from mass interception of electronic communication if this happens by coincidence. A new law, currently being adopted, will allow targeted collection against Danish citizens in certain cases, as mentioned earlier.

The data protection safeguards for the operations of DDIS are generally quite weak. Raw data can be shared with foreign intelligence services without any restrictions, even when the data is likely to contain information about Danish citizens, for example the contents of their electronic communication.

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. Foreign citizens cannot complain to the oversight board.

The right to privacy under the International Covenant on Civil and Political Rights and the European Convention of Human Rights applies to all citizens, whether Danish or foreign.

Denmark's national and international human rights obligations to promote, respect and protect the right to privacy must also apply to the operations of DDIS, irrespective of whether Danish or foreign citizens are affected.

C. Recommendations
We call upon the Government of Denmark to:

- Effectively investigate the credible allegations of unlawful surveillance by foreign intelligence agencies and the part played by the Danish security services;
- 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 current DDIS law.

Conclusion

I conclude by thanking you on behalf of IT-Political Association of Denmark for your attention.

For any further information, we kindly refer to the summary of our submission which outlines our recommendations and list of questions. We remain available should you wish any further details.

Thank you.