Udenrigsministeriet
Asiatisk Plads 2
1448 København K

Sendt per email til **upr2016@um.dk**

IT-Politisk Forening
c/o Jesper Lund
Carl Bernhards Vej 15, 2.tv
1817 Frederiksberg C

E-mail : bestyrelsen@itpol.dk
Web : http://www.itpol.dk

Dato : 25. september 2015

Comments on Denmark's second National Report for the Universal Periodic Review

The comments below from IT-Political Association of Denmark (IT-Pol) address the right to privacy which is not mentioned in the draft UPR National Report prepared by the Ministry of Foreign Affairs.

1. In the first cycle UPR review of Denmark, the issue of privacy was raised. In the National Report, Denmark noted *"thorough examination has been made of whether the rules [introduced by the new anti-terror packages] comply with Denmark's human rights obligations, including the obligation to guarantee every individual the right to privacy"* and *"found no reason to propose changes on the basis of the legal protection"*.

2. The National Report also noted that the decision not to propose any changes was criticised by, *inter alia*, civil society, and that the Government would take this criticism into consideration in its continued efforts to guarantee that the anti-terror legislation provides a basis for an effective combating of terrorism without compromising the fundamental rights of citizens.

3. In the first Universal Periodic Review for Denmark, the Netherlands recommended that Denmark should carry out an inclusive evidence-based evaluation of the Danish anti-terrorism legislation (recommendation 106.133).

4. This recommendation was not accepted by Denmark in 2011. However, in the 2014 mid-term Progress Report, the status of recommendation 106.133 was changed to ”under consideration”.

5. As far as IT-Pol is aware, the Government has not made any concrete steps towards initiating an evidence-based evaluation of the two major anti-terror packages adopted in 2002 and 2006.

6. On 19 February 2015, following the attacks in Paris and Copenhagen, the Government presented a new 12-point anti-terror plan, which has been informally referred to as anti-terror package III. Legislative proposals were submitted to Parliament for targeted surveillance of Danish citizens abroad by the Danish Defence Intelligence Services (DDIS) and increased access to Passenger Name Records (PNR) by the Danish Security and Intelligence Service (PET).

7. The target surveillance and PNR proposals lapsed when an election was called for 18 June 2015. IT-Pol expects that the new government will re-submit the proposals for targeted surveillance and PNR, and this is likely to be done before the second Universal Periodic Review in 2016.

8. Other proposals from a revised version of the February 12-point anti-terror plan are also likely to be part of the legislative plan presented by the Government when the next parliamentary session starts in October.

9. IT-Pol has been highly critical of the Danish anti-terror legislation, and especially the lack of a through evaluation. For example, the evaluation of the telecom data retention law has been postponed three times in 2010, 2012 and 2013. Before the election, the former government wanted to postpone the data retention evaluation for the fourth time.

10. The lack of interest by the Government in evaluating the existing anti-terror legislation, combined with a clear interest in proposing new

anti-terror legislation with increased surveillance powers, has negative implications for the right to privacy in Denmark.

11. After the revelations by Edward Snowden in June 2013, there has been increased focus throughout the World on the mass surveillance of electronic communication by intelligence agencies, such as the National Security Agency (NSA) in the United States and the Government Communications Headquarters (GCHQ) in the United Kingdom.

12. The Danish Government has refused to recognise the mass surveillance documented by the Snowden revelations as a threat to the privacy of Danish citizens. The Government has even refused to investigate specific cases of foreign spying in Denmark, documented by news media based on the Snowden files, claiming that there is no reason to believe that US intelligence agencies have been carrying out ”illegal surveillance” in Denmark.

13. A government has a clear obligation to protect its citizens, and their right to privacy, from foreign spying.

14. In 2013, the law governing the operations of DDIS was adopted by Parliament. This law gives DDIS almost unlimited powers to conduct any type of surveillance directed against foreign citizens with very limited oversight.

15. Furthermore, information about Danish citizens may be collected as ”raw data” (mentioned in the preparatory works of the DDIS law), as long as the DDIS collection is directed against conditions abroad.

16. The data protection safeguards for DDIS are very weak. For example, the right to access is denied for all citizens, Danish or foreign.

17. Danish citizens can complain to an oversight board (Tilsynet med Efterretningstjenesterne, TET), which will then investigate whether information about them is processed unlawfully. However, Danish

citizens will never be informed about any unlawful data collection or processing.

18. For foreign citizens, the data protection and oversight safeguards are even lower. Data on foreign citizens can be retained indefinitely, whereas there is an absolute 15-year limit for data on Danish citizens and raw data (which has not yet been processed).

19. Foreign citizens cannot complain to TET, and DDIS can share data on foreign citizens with other intelligence agencies, essentially without any restrictions.

20. Raw (unprocessed) data can also be shared with foreign intelligence services, even when the data is likely to contain information about Danish citizens, for example the contents of their electronic communication.

21. DDIS may not currently target Danish citizens when searching the raw data collection, but foreign partners of DDIS are not subject to these restrictions when receiving raw data from DDIS.

22. The 2014 annual report from TET on DDIS states that the electronic collection by DDIS includes very large quantities of ”raw data”.

23. Given the complete lack of restriction on sharing raw data with foreign partners, DDIS and hence Denmark is likely to play an active role in the European ”surveillance bazaar” which Edward Snowden gave testimony about to the European Parliament on 7 March 2014.

24. 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.

25. The data protection safeguards and oversight standards of DDIS are probably among the weakest in Europe.

26. 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.

27. Together with Privacy International, IT-Pol has submitted an UPR stakeholder report to the second cycle, where the above-mentioned issues are addressed, along with other concerns about the right to privacy in Denmark.