

Focus on digital homeworking

Focus investigation

Published: 2.11.2020



[FULL REPORT \(NL\)](#) ↗

[FULL REPORT \(EN\)](#) ↗

What we assessed and why

COVID-19 forced schools, universities, restaurants and offices to close their doors in March 2020. Where possible, working from home suddenly became the norm. Almost all of the 175 000 or so civil servants working for the ministries and High Councils of State had to work from home as far as possible, often very successfully. With trains empty, roads deserted, work continued from home. Civil servants collaborated and communicated by telephone, conventional network drives and e-mail, and increasingly via video-meetings, messaging apps and online collaborative platforms. Of course, collaborative ICT tools were nothing new, but now they were suddenly being used en masse for all kinds of new purposes. This raised many questions for users: Are video calls via Zoom secure? What information can I share in an app? How can I use my personal laptop securely for work? We identified risks in the use of collaborative ICT in central government. As a first step in investigating these risks, we set about finding out what ICT tools were used, how they were used and how their use was regulated.

What we found

We observed that the COVID-19 crisis had led to a rapid increase in teleworking in central government. This demanded enormous flexibility from ICT staff and support services. We paid tribute to the way ministries, the central government's chief information officer, individual civil servants and service providers, such as the ICT Shared Services Centre, had responded to the COVID-19 crisis.

We conducted a survey to obtain information on the ICT applications civil servants use when working from home. We found that communication on which collaborative ICT tools can be used needed to be clearer and easier to understand. A fifth of respondents said they were not aware of agreements on the use of collaborative ICT tools; 22 % were not satisfied with communication on these agreements. The greatest uncertainty concerned the use of messaging apps, such as WhatsApp and online collaboration platforms such as Microsoft Teams, SharePoint and Dropbox.

7 % of respondents who use WhatsApp and 16 % of respondents who use private email had also shared confidential information without permission. One reason for this was that civil servants sometimes did not know which applications they were allowed to use. For example, the central government's intranet states that WhatsApp may be used for work under certain conditions. However, several ministries explicitly forbid the use of this messaging app.



Dissatisfaction with the capabilities offered by the available ICT tools is one of the main reasons for going against these agreements by using apps that are not recommended. Ministers, state secretaries and senior civil servants also do not always use the prescribed and available secure ICT tools, even though their use of ICT tools sets an example for the rest of the organisation. Ministers, state secretaries and senior civil servants sometimes prefer popular messaging apps, such as WhatsApp, less secure tablets and smartphones because they are more convenient, faster and more user-friendly than highly secure tools.

Our investigation revealed an example of this. In spring 2020, one of the ministries set up an ultra-secure environment for video-meetings at the request of the central government's chief information officer. This environment was provided for confidential communication between ministers and state secretaries, but it was not used.

What we concluded

Our investigation shows that central government has to take steps to make its use of messaging apps and mobile phones more secure. We see their use as the biggest risk to information security and privacy. If the recommended ICT tools are not used, or are used incorrectly, information can fall into the wrong hands.

Some civil servants in central government see the need for clearer communication on the secure use of collaborative ICT tools, such as messaging apps and online meeting services. Some civil servants use WhatsApp and private email to share confidential work-related information, thus failing to comply with their organisations' security guidelines.

These observations led to a follow-up investigation in our 2020 annual financial audit on information security in central government. We looked specifically at central government's risk and incident management in relation to WhatsApp and the various video conferencing tools in use. We have published the results in May 2021.