37th Meeting of Senior Officials from Centres of Government

Leading the Digital Transformation from the Centre of Government

Dublin, Ireland, 8-9 November 2018

Summary
Summary of the discussions

The 2018 meeting of the OECD Network of Senior Officials from Centres of Government focused on “Leading the Digital Transformation from the Centre of Government”. Hosted by the Irish Government and chaired by Mr. Martin Fraser, Secretary-General to the Government, the meeting brought together over 30 OECD member and partner countries. The three main sessions looked at anticipating trends and building a strategic response to digital transformation, data governance, and cybersecurity.

Digitalisation, and the interconnectedness it brings, is transforming the workplace, the economy and society in complex, interrelated and often unpredictable ways. However, governments are not keeping up with the pace of change. There is a growing gap between people’s experiences as consumers and their experiences as citizens. A major challenge for governments is to try to close this gap, in terms of how citizens interact with the state and receive public services. Going beyond, government must also try to anticipate change and its implications.

In most countries, the centre of government is playing a major role in ensuring a strategic and co-ordinated approach to digital transformation. Even if, in some cases, formal responsibility for digital issues is not (or is no longer) placed in the centre, the latter is still closely involved in many strategic aspects of the government’s response. Digital is “everywhere”, and cannot be entirely separated from other policy areas. Both centralisation and a more decentralised approach to managing digital transformation have their advantages. Decentralisation can allow ministries, agencies and lower levels of government to move quickly to adopt new technologies to improve efficiency or productivity. But it can make it more difficult to achieve the co-ordinated, comprehensive approach that digital government requires.

An important aspect of anticipating and preparing for change is recognizing that tomorrow’s technology may be radically different from today’s. This means that not only should laws and policies be designed with this in mind, but that the regulatory process itself needs to adapt to enable more frequent, even continuous, revision to keep pace with accelerating technological change. For instance, artificial intelligence (AI) will oblige governments to regulate human-algorithmic relationships, such as in the case of liability for accidents involving self-driving cars. AI, the Internet of Things and other new technologies are prompting a discussion of who “owns” data and the rules governing it. Digital coding and algorithms may need to be treated the same way we treat law, with the state playing a role in how coding is done to ensure that it supports transparency and a level playing field, does not build biases into the system, and aligns with national values.

Staying abreast of change and adapting policies and processes means that government needs new skills. Countries often address the skills gap through a mix of building capacity in-house or bringing in expertise from outside, sometimes for specific, fixed-term projects. Some have special units or advisors in the centre who focus on future trends and challenges. Governments are also looking to the private sector for ideas or tools and processes it can adapt or use directly. For example, the banking and financial
sector is a leader in identity management, risk assessment, fraud, etc. At the same time, centres of government are struggling to attract the talented, skilled people they need in an increasingly competitive digital economy job market.

The need to promote innovation and to act quickly can run counter to the public administration’s tendency toward risk aversion and lengthy policy formulation and implementation processes. In response, some governments are bypassing the strategy phase in some areas (e.g. applying AI). Rather than “think-tanks” they are creating “do-tanks”, innovation labs and regulatory “sandboxes” to allow innovations to be tested in a light regulatory environment. But navigating the trade-offs between taking certain risks and not stifling innovation or missing opportunities is not easy, especially when public failures or problems can quickly overshadow government’s successes. It is also important to try to close the digital divide, by ensuring that citizens get the digital skills they need, or can still access services in more traditional ways. Some countries have created “digital mailboxes” for citizens for their interactions with the state, and many are trying to implement “ask only once” policies, whereby citizens and businesses have to supply a piece of information only once to the government.

Obstacles to such policies can be raised by agencies’ reluctance to share data that they consider under their “guardianship”, and some citizens do not necessarily want a government agency (e.g. social service provider) to share their data with another (e.g. tax authority). There is also a tension between a citizens’ right to services (and responsibility as a citizen) and his or her “right to be forgotten” or removed from databases. To overcome such obstacles, the state must bolster trust and encourage co-operation both inside and outside the administration through open communication and education.

In order to build trust, it is crucial to develop a coherent and convincing political narrative around digitalisation that balances the risks and threats with the positive benefits brought about by the ongoing digital transformation. The centre of government can play an important role in crafting this narrative and communicating it to the public as well as within government.

The “dark sides” of digitalisation – cyber insecurity and cybercrime – have helped shift digital governance firmly to the centre of the political agenda. Countries are seeing success in reducing the impact of cyber-attacks – such as reducing the time it takes to remove fake government websites – but the number and sophistication of such attacks continues to increase, requiring continued vigilance, mobilisation of resources and new skills in the public sector. Government are seeking to be more proactive, and go beyond passive defence to “comprehensive cyber deterrence”. Partnering with industry is an important part of these efforts. Furthermore, stronger international co-operation, particularly in the area of cybersecurity, is crucial, both in terms of sharing information and working across borders to counter threats.

As a complement to the discussion of the role of the centre in supporting the digital economy, the OECD presented the results of its 2017 international survey on policy making, leadership and capacity at the centre of government. This survey highlights evolutions in the way that the centre of government performs its key functions. With respect to the issue of leadership and policy skills at the centre, the OECD suggested that it could play a role in providing tailored capacity-building support and training to interested administrations.

The 2019 meeting will be hosted by Iceland’s Prime Minister’s Office in Reykjavik.