TOOP and the GDPR: how the once-only principle contributes to a higher level of data protection in the EU

As any European with an e-mail address has undoubtedly noticed, on the 25th of May 2018, the new European legal framework for personal data protection, the General Data Protection Regulation or 'GDPR', became applicable across the EU. The GDPR has raised the bar for the protection of personal data in a number of areas, including with respect to transparency and the requirements for a legally valid consent. This is the main reason why the average citizen has now received countless e-mails to inform them of who is processing their data, why, and to determine whether that citizen still agrees to the use of their data.

Data protection is of course a critical concern in once-only use cases as well. Any once-only service essentially revolves around re-using data held by one administration, by providing it to another administration directly. This is hugely beneficial for the end user: it is easier, reduces time and effort, and also decreases the chance of mistakes since existing trustworthy data doesn't have to be manually re-entered over and over again.

But once-only also means that new data protection challenges must be addressed. Transparency towards the user is of course very important: a user should be aware of exactly which data would be exchanged, who will be receiving it, and for which purposes. Legitimacy of the data exchange is another key issue: data which is not already available, either publicly or at least to the receiving administration, should only be exchanged after the user has consented to it. Exchanges must also be secure: the data which reaches a public administration should be exactly the same as the data held in the original database, and it must be possible to detect any problems. Furthermore, to ensure that the processing is fair, the user should have the possibility to preview the data before it is sent to its new recipient. This allows users to examine precisely which information they are making available, and allows them to change their minds before problems can occur. Finally, accountability plays a central role: if a mistake happens, it must be possible in all cases to determine where exactly the problem lay, so that it can be corrected and avoided in the future.

The TOOP project was build precisely to address these data protection requirements, which have been made more explicit in the proposed Single Digital Gateway Regulation (SDGR), that clarifies how the more general principles of the GDPR apply in a once-only context. TOOP is therefore an example of the application of the GDPR's privacy by design principle: the infrastructure which is being created and piloted in TOOP has been designed from the ground up to ensure that it supports and facilitates GDPR compliance, rather than creating new risks or bolting on safeguards afterwards. For this reason too, the TOOP project is conducting and maintaining data protection impact assessments throughout the duration of the project, so that any existing or emerging risks can be identified and mitigated. In this way, TOOP contributes to the application of the GDPR in once-only initiatives, and effectively raises the bar for data protection in cross-border data exchanges.

Hans Graux