Message on the occasion of the 17th Data Protection Day,
28 January 2023

Jean-Philippe WALTER, Council or Europe Data Protection Commissionner

Respecting data protection right weakened in the context of international crises

On 28 January 2023, we celebrate the 17th Data Protection Day. At the Council of Europe, the beginning of 2023 is marked by the entry into force of a new regulation on data protection adopted by the Committee of Ministers on 15 June 2022. This regulation governs the processing of personal data of the Organisation. It finally enables the Council of Europe to adopt modern legislation that is largely in line with the requirements of Convention 108+. In particular, it strengthens the rights of data subjects, clarifies the obligations of controllers, and consolidates the powers and competences of the Data Protection Commissioner as an independent supervisory authority.

This 17th Data Protection Day is unfortunately marked by the gloom and uncertainties related to the international situation and in particular to the war, the climate crisis, the economic and financial crises that impact the daily lives of many of us or related to the deterioration of social cohesion or health systems. This bleak picture has implications for our human rights and fundamental freedoms, including the right to data protection. In this climate of uncertainty and tension, there is indeed a strong temptation to introduce measures restricting our rights and freedoms and to resort too conveniently to surveillance technologies that could get to unwise processing of personal data. All the ingredients are there for an increased risk of definitively switching to a surveillance society, putting pressure against the respect for human rights, rule of law and democracy. Democracies are currently in sharp decline around the world. According to Freedom House, today only 20% of the world's population lives in a democratic State. This is very sobering.

The danger of this slide towards widespread surveillance is not the exclusive preserve of the State. It is also linked to the fast-paced digitalisation of society and the inexorable reckless imposition by the digital technology giants of the use of information and communication technologies in all our actions and interactions in everyday life, at the risk of leaving aside many citizens around the world. These giants feed on the countless data that we deliver to them over and over and, which allows them to profile us, to guide our choices and behaviours, to manipulate us and finally to decide for us. This "surveillance capitalism" has taken possession of our data to claim for itself the right to manage our lives. The tremendous expanding of artificial intelligence systems is another challenge to the respect of our human rights and fundamental freedoms. While the digitalisation of our societies and the use of artificial intelligence have many positive aspects and seem irreversible, they present many risks that should not be underestimated both for the respect of our privacy and for our individual and societal security. Safeguards exist, but they must be applied.

- Thus, it is urgent that the development of artificial intelligence systems be regulated by robust legislation. The entry into force of Convention 108+, which we hope is near, and the rapid adoption of a Convention on artificial intelligence will contribute to this.

- Digitalisation, the use of artificial intelligence or the use of any other surveillance technologies must be accompanied and preceded by a broad democratic and public debate.

- Education and awareness of digital technology and the use of information and communication technologies for all segments of the population must be developed and highlighted so that everyone can regain control of their private lives, become more critical and decide freely, responsibly and knowingly about their actions without their decisions affecting the choice of others.

- IT architectures must be redesigned to better preserve human rights and fundamental freedoms and better guarantee the security of data and infrastructure. This implies that we move away from an all-digital and all-connected world for a more differentiated approach, creating non-discriminatory or non-dissuasive alternatives.

- The activities of the IT giants must be better regulated.

- Laws must be enforced and their application better supervised.

The role of data protection authorities (supervisory authorities) is therefore crucial. They are actually responsible for ensuring compliance with legal provisions on data protection and, where appropriate, punishing violations. They have a preventive and, if necessary, repressive role. They must be in a position to conduct investigations, establish facts, investigate complaints and take decisions, and impose sanctions. They must be able to provide advice to the various actors involved in the processing of personal data, give opinions, provide guidance and be able to anticipate risks, in particular through technology watch actions. They also have a role to play in information, awareness-raising and training. While performing their functions, they are also called upon to cooperate with each other or with other supervisory authorities. This implies that supervisory authorities have sufficient resources, including financial means, to carry out their tasks and exercise their powers efficiently, effectively and independently. They must have sufficient qualified and experienced staff with legal, computer, economic, social and information skills.

There is an urgent need to act and move towards a society that is more respectful of human rights and fundamental freedoms, based on the rule of law and upholding democracy. It is not too late. This 17th Data Protection Day is an opportunity for society as a whole to revive awareness of the challenges of digitalisation, to discuss them and to initiate the necessary steps to give back citizens control over their private lives and avoid becoming definitively "digital slaves". A digital summit bringing together politicians, tech companies, the scientific world and civil society is an avenue to explore.

Faced with security challenges, our States must avoid the trap of ill-considered surveillance measures, putting fundamental rights and freedoms, as well as the instruments of the rule of law, on hold. The defence of public interests, however legitimate they may be, cannot be opposed to respect for data protection. One cannot go without the other.