COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

SUMMARIES OF THE COUNCIL OF EUROPE TREATIES

The summaries available hereunder are designed to meet a practical need, that of supplying the public at large with concise descriptions of the Council of Europe treaties. The summaries are necessarily short and can therefore only give a first introduction to the main features of each treaty.

Subject-matter: DIGITAL DEVELOPMENT AND GOVERNANCE

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), open for signature, in Strasbourg, on 28 January 1981.

Entry into force: 1 October 1985.

This Convention is the first binding international instrument which protects the individual against abuses which may accompany the collection and processing of personal data and which seeks to regulate at the same time the transfrontier flow of personal data.

In addition to providing guarantees in relation to the collection and processing of personal data, it outlaws the processing of "sensitive" data on a person's race, politics, health, religion, sexual life, criminal record, etc., in the absence of proper legal safeguards. The Convention also enshrines the individual's right to know that information is stored on him or her and, if necessary, to have it corrected.

Restriction on the rights laid down in the Convention are only possible when overriding interests (e.g. State security, defense, etc.) are at stake.

The Convention also imposes some restrictions on transborder flows of personal data to States where legal regulation does not provide equivalent protection.

* * *

Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows (ETS No. 181), open for signature, in Strasbourg, on 8 October 2001.

Entry into force: 1 July 2004.

The text will increase the protection of personal data and privacy by improving the original Convention of 1981 (ETS No. 108) in two areas. Firstly, it provides for the setting up of national supervisory authorities responsible for ensuring compliance with laws or regulations adopted in pursuance of the convention, concerning personal data protection and transborder data flows. The second improvement concerns transborder data flows to third countries. Data may only be transferred if the recipient State or international organisation is able to afford an adequate level of protection.

* * *

Convention on Cybercrime (ETS No. 185), open for signature, in Budapest, on 23 November 2001.

Entry into force: 1 July 2004.

The Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception.

Its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation.

* * *

Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189), open for signature, in Strasbourg, on 28 January 2003.

Entry into force: 1 March 2006.

This Protocol entails an extension of the Cybercrime Convention's scope, including its substantive, procedural and international cooperation provisions, so as to cover also offences of racist or xenophobic propaganda. Thus, apart from harmonising the substantive law elements of such behaviour, the Protocol aims at improving the ability of the Parties to make use of the means and avenues of international cooperation set out in the Convention (ETS No. 185) in this area.

* * *

Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223), open for signature, in Strasbourg, on 10 October 2018.

Entry into force: Ratification by all Parties to the Protocol, or, as from 11 October 2023, once 38 Parties to the Convention have ratified the Protocol.

The aim of the Protocol of amendment is to modernise and improve the Convention (ETS No. 108), taking into account the new challenges to the protection of individuals with regard to the processing of personal data which have emerged since the Convention was adopted in 1980.

The modernisation of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, the only existing legally binding international treaty with global relevance in this field, addresses the challenges to privacy resulting from the use of new information and communication technologies, and strengthens the convention's mechanism to ensure its effective implementation.

The Protocol provides a robust and flexible multilateral legal framework to facilitate the flow of data across borders while providing effective safeguards when personal data are being used. It constitutes a bridge between different regions of the world and different normative frameworks, including the new European Union´s legislation that will become fully applicable on 25 May 2018 and which refers to Convention 108 in the context of transborder data flows.

Some of the innovations contained in the Protocol are the following:

- Stronger requirements regarding the proportionality and data minimisation principles, and lawfulness of the processing;
- Extension of the types of sensitive data, which will now include genetic and biometric data, trade union membership and ethnic origin;
- Obligation to declare data breaches;
- Greater transparency of data processing;
- New rights for the persons in an algorithmic decision making context, which are particularly relevant in connection with the development of artificial intelligence;
- Stronger accountability of data controllers;
- Requirement that the "privacy by design" principle is applied;
- Application of the data protection principles to all processing activities, including for national security reasons, with possible exceptions and restrictions subject to the conditions set by the Convention, and

in any case with independent and effective review and supervision;
- Clear regime of transborder data flows;
- Reinforced powers and independence of the data protection authorities and enhancing legal basis for international cooperation.

* * *

Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224), open for signature, in Strasbourg, on 12 May 2022.

Entry into force: The Protocol will enter into force following five ratifications.

Considering the proliferation of cybercrime and the increasing complexity of obtaining electronic evidence that may be stored in foreign, multiple, shifting or unknown jurisdictions, the powers of law enforcement are limited by territorial boundaries. As a result, only a very small share of cybercrime that is reported to criminal justice authorities is leading to court decisions.

As a response, the Protocol provides a legal basis for disclosure of domain name registration information and for direct co-operation with service providers for subscriber information, effective means to obtain subscriber information and traffic data, immediate co-operation in emergencies, mutual assistance tools, as well as personal data protection safeguards.

* * *

Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225), open for signature, in Vilnius, on 5 September 2024.

Entry into force: The Convention will enter into force following 5 Ratifications including at least 3 member States of the Council of Europe.

The *Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law* is intended to address specific challenges which arise throughout the lifecycle of artificial intelligence systems and encourage the consideration of the wider risks and impacts related to these technologies including, but not limited to, human health and the environment, and socio-economic aspects, such as employment and labour.

The provisions of this Convention aim to ensure that activities within the lifecycle of artificial intelligence systems are fully consistent with human rights, democracy and the rule of law.

* * *