

Declaration

Strengthening Regional Cooperation on Data Protection, Artificial Intelligence and Health Data

ANNUAL MEETING OF CENTRAL AND EASTERN EUROPE DATA PROTECTION AUTHORITIES

Zadar, Croatia | 24–26 September 2026

Preamble:

Artificial intelligence and the growing use and exchange of health data are transforming public services, healthcare, research and everyday life. Their benefits depend on respect for human dignity, privacy and the protection of personal data, non-discrimination and effective remedies. Protecting individuals and enabling responsible innovation are mutually reinforcing objectives that require safeguards to be embedded in the design, deployment and oversight of digital systems.

The Central and Eastern Europe Data Protection Authorities (CEEDPA) initiative brings together authorities operating within and outside the European Union, under different legal frameworks and institutional arrangements. Its enduring value lies in direct dialogue, mutual assistance and the exchange of practical experience. These relationships support convergence towards high standards of protection while respecting the independence and responsibilities of each authority.

Building on this tradition, the Annual Meeting in Zadar provides an opportunity to renew our common commitment and connect it to practical work on artificial intelligence, health data governance and effective supervision. The Council of Europe's Convention 108+ offers a shared reference for cooperation across the region, alongside applicable national and European Union law.

Recognising that:

Risks arising from digital technologies and cross-border data processing cannot be addressed effectively by authorities acting in isolation, and differences in legal frameworks should encourage dialogue and mutual learning;

Security risk assessments, data protection impact assessments (DPIAs) and fundamental rights impact assessments (FRIAs) serve complementary purposes, but have distinct scopes, legal requirements and consequences;

The sensitivity of health data, and the consequences of their misuse for individuals and groups, require effective safeguards throughout their collection, access, exchange and reuse;

Independent, adequately resourced and accessible supervisory authorities are essential to public trust, effective enforcement and the practical exercise of individuals' rights.

Recalling:

The Warsaw Declaration on Future Cooperation of 17 December 2001, the Smolenice Declaration on Future Cooperation of 24 May 2005, the Kazimiersk Declaration on Future Cooperation of 3 June 2008, and the Declaration on Mutual Assistance and Enhanced Cooperation of 2–3 April 2014;

The principles reflected in the European Convention on Human Rights, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108, ETS No. 108), its Additional Protocol (ETS No. 181), its Amending Protocol (CETS No. 223), the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225), and the Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine (Oviedo Convention, ETS No. 164);

The principles set out in Recommendation CM/Rec(2019)2 of the Committee of Ministers to member States on the protection of health-related data;

The relevance, within their respective scope of application, of the Charter of Fundamental Rights of the European Union, Regulation (EU) 2016/679 (GDPR) and Regulation (EU) 2024/1689 (AI Act) and Regulation (EU) 2025/327 on the European Health Data Space (EHDS);

The contributions of the Council of Europe in the field of artificial intelligence and human rights, including through the Methodology for assessing the risks and impacts of artificial intelligence systems from the perspective of human rights, democracy and the rule of law (HUDERIA Methodology) and the HUDERIA Model: Context-Based Risk Analysis (COBRA), as well as those of the European Data Protection Board, the European Data Protection Supervisor and other relevant stakeholders, to the development of practical responses to emerging challenges.

The participating data protection authorities of the Central and Eastern Europe initiative hereby declare their commitment, within their respective mandates and applicable legal frameworks, and having regard to the scope and application dates of the instruments concerned:

1. To strengthen common foundations and regional cooperation.

To promote high standards of protection throughout the region, support broader adherence to Convention 108+ and encourage its prompt ratification. Cooperation should support authorities undertaking legal or institutional reforms and enable all participating authorities to contribute their experience.

2. To promote coherent and substantive assessment of risks arising from AI systems.

In particular:

- (a) Encourage coordinated assessment processes using a common factual and evidential foundation, including the system's purpose, deployment context, data flows and affected persons;
- (b) Promote assessment of lawfulness, necessity, proportionality and less intrusive alternatives from the earliest stages of planning and procurement and before deployment, together with

the risks to individuals and groups. Encourage the timely involvement of data protection officers and, where appropriate, guidance from or consultation with competent data protection authorities, particularly in public procurement. Security measures and favourable risk scores cannot substitute for a lawful basis or justify processing that infringes fundamental rights;

- (c) Encourage assessment throughout the system lifecycle, with documented responsibilities, evidence of the effectiveness of safeguards and review when systems, purposes, data or deployment contexts change. Assessments should lead to concrete decisions to proceed lawfully, modify, suspend or refrain from deployment, and to prior consultation or other regulatory procedures where required;
- (d) Exchange experience with practical assessment methods, including HUDERIA and relevant privacy and human rights impact assessment tools, recognising that their use must be adapted to the context and does not in itself establish legal compliance.

3. To keep affected individuals and communities at the centre of AI governance.

In particular:

- a) To promote meaningful participation of affected persons and relevant stakeholders, with particular attention to children and persons in vulnerable situations. Assessments should consider discriminatory, cumulative and group impacts, especially where AI influences access to education, healthcare, social protection or other essential services.
- b) To encourage understandable information, effective human oversight and accessible mechanisms to challenge outcomes, correct errors and obtain remedies. Human oversight should be exercised by persons with the competence, information, time and authority to question and, where appropriate, disregard or reverse an AI-generated output.

4. To advance trustworthy governance and responsible use of health data.

In particular:

- a) To promote the processing of health-related data primarily in the public interest, notably to improve the health and well-being of individuals and society, while safeguarding individual rights and respecting the primacy of the interests and welfare of the individual over the sole interests of society or science. Such processing should comply with applicable legal requirements and rigorous ethical safeguards, taking account of the Oviedo Convention and Recommendation CM/Rec(2019)2. To exchange experience and promote safeguards for the use and sharing of health data in healthcare, research and other lawful activities, with particular attention to:
- b) Making individuals' rights effective through clear information, accessible procedures and reliable arrangements for authentication and representation, including practical means to access and seek rectification of their health data and exercise other rights under applicable law;
- c) Ensuring that further use of health data rests on a lawful basis and clearly defined purposes, respects purpose limitation and data minimisation, and provides effective safeguards against unauthorised use, discrimination and other harms;

d) For research and other further uses, promoting the use of anonymised data where the purpose can be achieved in that way and, where personal data are necessary, safeguards appropriate to their sensitivity and the risks, including pseudonymisation, restricted access, secure processing, logging and scrutiny of disclosed results. Safeguards should address re-identification risks, including those arising from linking datasets;

e) Promoting transparency and accountability in arrangements for sharing health data, including clear information about the datasets, intended uses and conditions of access, while protecting confidentiality and ensuring that making a dataset discoverable does not itself authorise its use;

f) Clarifying responsibilities and strengthening practical cooperation among data protection authorities, competent health authorities and other relevant bodies, taking account of national institutional arrangements. Such cooperation should support effective complaint handling, coordinated responses to incidents and secure information exchange, while preserving the powers and independence of the authorities concerned.

5. To strengthen supervisory independence, capacity and effectiveness.

In particular:

a) To call upon governments and legislatures to safeguard the institutional independence of data protection authorities and provide human, technical and financial resources commensurate with their responsibilities, including new tasks arising from digital regulation. Authorities should be involved at an early stage in relevant legislative and institutional developments.

b) To exchange experience on multidisciplinary expertise, staff training, supervisory priorities and the evaluation of our work. Such evaluation should consider the quality, timeliness and practical effect of supervision on compliance and individuals' rights, taking account of differences in mandates, resources and national contexts.

6. To make cooperation practical, inclusive and sustainable.

In particular:

a) To facilitate direct professional contacts, voluntary peer exchanges and mutual assistance, including cross-border matters where legally permitted. Information sharing must respect applicable confidentiality, data protection and international transfer requirements.

b) To build on existing cooperation channels and the work of the Council of Europe, the Spring Conference, the EDPB, the EDPS and other relevant stakeholders, avoiding unnecessary duplication and making useful experience available to authorities throughout the initiative.

This Declaration renews the commitment of the participating authorities to translate shared principles into effective protection for individuals. Through practical cooperation on artificial intelligence and health data, we seek to strengthen accountability, public trust and respect for fundamental rights throughout Central and Eastern Europe.

Further to these commitments, the participating authorities resolve on a voluntary basis and subject to their mandates and available resources, to:

- a) Share the agreed, non-confidential conclusions and reusable materials from the Zadar workshops, including practical lessons on AI assessments and cooperation in health data governance;
- b) Take stock of progress at the next Annual Meeting, based on voluntary contributions, and agree priorities for further cooperation;
- c) Disseminate the adopted Declaration through participating authorities' websites and relevant cooperation networks and bring it to the attention of competent national institutions.