GANHRI Annual Conference 2026
Outcome Statement

The role of National Human Rights Institutions in promoting and protecting human rights in the digital space

Global context and call to action:

1. On 1 April 2026, we, the National Human Rights Institutions (NHRIs) from all regions, gathered in Geneva for the Annual Conference on the role of NHRIs in promoting and protecting human rights in the digital space, held in the context of the Global Alliance for National Human Rights Institutions (GANHRI) 2026 Annual Meeting.

2. We are gathered at a time of profound instability when human rights protections are under growing pressure and the international human rights system faces serious challenges.

3. In this context, we affirm that human rights must be at the core of the digital transformation. Digital technologies increasingly shape the enjoyment of human rights across all areas of life, with significant implications for civic space, access to information, public services, justice and participation in public affairs.

4. We recognize that digitalisation can contribute to the realization of human rights. It can expand access to information and services, facilitate communication, support inclusion, improve institutional effectiveness and strengthen engagement with and between rights-holders.

5. At the same time, in many national contexts, digitalisation is advancing more rapidly than the development of legal safeguards, institutional capacity, public awareness and effective oversight. This creates a heightened risk that rights-infringing practices become normalised before they are adequately understood, regulated or remedied. Across all regions, we observe serious threats: unlawful surveillance, misuse of personal data, algorithmic opacity, discriminatory profiling, online harassment and abuse, manipulation of information, and the use of digital tools to intimidate, monitor or silence critical voices. These developments affect the enjoyment of rights, including but not limited to

privacy, freedom of expression, equality and non-discrimination, participation, due process and access to effective remedy. We also note the rise of automated decision-making which can pose serious threats when applied in situations where human rights are at stake.

6. We reaffirm that international human rights law applies fully in the digital sphere, and that the same rights people enjoy offline must be protected online. This principle must guide the design, development, deployment and use and regulation of digital technologies, including artificial intelligence.

7. We note the growing number of international and regional initiatives addressing digital governance, including the Global Digital Compact and other multilateral processes. These initiatives must be firmly grounded in international human rights law and informed by the expertise and engagement of NHRIs.

8. We are particularly concerned that digital harms can exacerbate existing inequalities, disproportionately affecting individuals and communities already subject to discrimination, exclusion or heightened vulnerability.

9. We note that there are distinct gendered risks in digital environments, including technology-facilitated gender-based violence, non-consensual intimate imagery, and online harassment. Digital governance frameworks, legal protections and remedies must integrate a gender perspective and effectively address these harms.

10. We recognise that children, persons with disabilities, older persons, minorities, Indigenous Peoples, migrants, stateless communities, women and girls, persons living in poverty, LGBTQI+ persons, and human rights defenders, including NHRIs and journalists, among others, face heightened exposure to digital exclusion, surveillance, abuse or discriminatory impacts.

11. We note that digital technologies and their underlying business models often operate across borders, while oversight mechanisms, accountability and access to remedy remain uneven and fragmented. This gap demands stronger domestic safeguards, enhanced cross-border and international cooperation, and continued engagement in emerging digital governance processes.

12. We are particularly concerned about discriminatory profiling and algorithmic discrimination, which can exacerbate existing inequalities and disproportionately affect individuals and communities already facing exclusion. These harms can occur in automated decision-making systems used in public

services, such as, policing, education, healthcare, migration, and other areas that have a direct impact on human rights.

13. We recognise that digital technologies could severely harm the environment and exacerbate climate change, which in turn undermines the rights of individuals and communities already in situations of climate-vulnerability. We particularly note significant environmental footprint of AI data centres and their growing contribution to water scarcity.

14. In this context, we call on States to ensure that digital transformation is firmly grounded in international human rights law and international environmental law guided by dignity, equality, non-discrimination, legality, necessity, proportionality, transparency, accountability and access to effective remedies.

15. We call on States to adopt and strengthen comprehensive legal and policy frameworks that address the human rights implications of digital technologies coherently across all sectors. Such frameworks must provide effective protection against unlawful or arbitrary surveillance, privacy interference, discriminatory automated decision-making, censorship, data misuse, online violence and other digital harms.

16. We stress that the use of artificial intelligence and other digital systems, particularly by public authorities, must remain subject to clear legal frameworks, ex ante safeguards, meaningful human oversight and independent scrutiny. Transparency, explainability and accountability must be guaranteed, especially where such systems affect access to public services, justice, migration procedures, policing, social protection, education, healthcare or other areas with significant consequences for rights. This is particularly important where States deploy digital identity systems, integrated public service platforms, civil registration systems, interoperable databases or other large-scale public sector data infrastructures. Where rights are affected, individuals must be able to understand decisions, contest them and obtain timely, appropriate redress.

17. We are concerned about the growing use of AI and neurotechnology in military and security management contexts, including autonomous and predictive technologies. Such applications carry risks to life, liberty and due process. There must be rigorous human rights safeguards and oversight, as well adherence to international humanitarian law.

18. We note that effective oversight requires coordination between NHRIs, data protection authorities, equality bodies, regulators and other competent oversight institutions. We call for mandatory human rights impact assessments

in relation to digital technologies used by public authorities, particularly in contexts where they may create serious risks or have far-reaching consequences for individuals and communities. Such assessments must help identify, prevent and mitigate harm, and inform decisions on about technology design, development, deployment, appropriateness and continued use, and address risks such as discriminatory bias and other adverse human rights impacts.

19. We stress that digitalisation must not become a barrier to rights. States have an obligation to ensure that digital public services and systems are accessible, inclusive, safe and affordable, and should maintain effective non-digital alternatives to guarantee that no one is excluded from services, participation or remedies based on disability, age, poverty, geography, language or limited digital access or skills.

20. We call on States and relevant actors to take stronger, coordinated measures to close digital divides within and among countries and to promote meaningful, equitable and non-discriminatory access to digital infrastructure, tools and information. Such efforts should also include strengthening human rights-based digital literacy, including online safety, through education and public awareness initiatives.

21. We further call on States to protect freedom of expression and access to information in digital environments. Responses to harmful online content must remain fully consistent with international human rights law and must not be used as pretexts for censorship, arbitrary restriction or the narrowing of civic or democratic space. States should also refrain from funding or promoting, through digital communications, misinformation aimed at undermining human rights, the rule of law, and democratic stability. Content moderation policies and practices should likewise be guided by clear, transparent and non-discriminatory rules, with effective opportunities for review and appeal.

22. We recall, in line with the Marrakech Declaration, our role in protecting and expanding civic space and in supporting those who defend human rights. This responsibility extends fully to the digital sphere, where participation, advocacy and public expression increasingly occur. We therefore express our deep concern over the misuse of digital technologies to intimidate, surveil, harass or silence human rights defenders, journalists, and civil society actors.

23. We call on States to refrain from imposing internet shutdowns and other broad disruptions to digital communications, including in electoral and protest contexts, where such measures impede access to information, restrict participation and interfere with fundamental rights.

24. We recall our commitments under the Kyiv-Copenhagen to assess the impacts of the use of new and emerging technologies in relation to deprivation of liberty, the rule of law, access to justice and the prevention of torture and other ill-treatment. This includes the use of artificial intelligence in decision-making and facial recognition technologies by police and security services, as well as the proliferation of online hate and disinformation.

25. We stress that private actors, including technology companies, digital platforms and especially very large online platforms (VLOPS), data processors and developers and deployers of AI systems, also bear responsibility to respect human rights. In line with the UN Guiding Principles on Business and Human Rights, they should exercise human rights due diligence, identify and address adverse impacts, regularly assess high-risk AI systems, and ensure meaningful transparency and accountability in relation to their systems, operations and business practices. They should also ensure meaningful and effective access to remedy for individuals whose rights are adversely affected by their technologies, including through accessible and effective complaint mechanisms and cooperation with competent oversight bodies.

Our commitments:

26. In this context, National Human Rights Institutions play a unique role as independent state bodies mandated to promote and protect human rights. Through their advisory functions, monitoring mandates, complaints-handling powers, engagement with international mechanisms, and role in the teaching of, and research into, human rights. NHRIs are well positioned to assess the human rights implications of digital technologies, prevent and mitigate digital harms, support rights-based governance, and provide accessible remedies for individuals affected by digital harms.

27. As independent institutions established in accordance with the Paris Principles and entrusted with broad mandates to uphold human rights, we reaffirm our commitment to promoting and protecting human rights in the digital space, in accordance with our respective mandates, priorities, capacities, and national contexts.

28. We will strengthen our efforts to monitor and report on the human rights implications of digital technologies at the national, regional and international levels. This includes assessing and monitoring developments in online civic space and the situation of human rights defenders and others facing heightened risk in digital environments.

29. We will continue to examine how digitalisation affects the enjoyment of rights, including but not limited to privacy, freedom of expression, equality and non-discrimination, participation, due process and access to justice. We will seek to integrate these concerns into our engagement with States, parliaments, oversight bodies, regional mechanisms and international human rights processes.

30. We will continue to provide independent expert advice to governments and parliaments on legislation, policies and regulatory frameworks relating to digital technologies and artificial intelligence. Our guidance will seek to ensure that emerging digital technologies are developed and deployed in line with human rights standards and the principles of inclusivity, fairness and accountability.

31. We will advocate for legal, policy and institutional frameworks that place human rights at the centre of digital governance, including in relation to the design, development, deployment and use of artificial intelligence. These frameworks should promote transparency, accountability, meaningful human oversight and accessible and effective remedies.

32. We will receive, analyse and follow up on complaints concerning human rights harms associated with digital technologies. This may include cases involving online intimidation, hate speech, surveillance, exclusion, abuse or restrictions affecting children, human rights defenders and other rights-holders in situation of vulnerability.

33. We will also work to ensure that individuals affected by digital technology related harms, including harms arising from automated decision-making or content moderation practices, have accessible, effective and timely avenues for redress.

34. We will work to enhance our own capacity to assess and respond to the human rights implications of artificial intelligence and other emerging digital technologies, through measures such as training, access to expertise, exchange of practice and cooperation across regions and jurisdictions.

35. We will contribute to greater public understanding of human rights in the digital space, including by supporting rights-holders to develop digital literacy, identify risks, understand available protections and seek remedies.

36. We will seek to use digital tools within our own institutions in ways that are secure, accessible, inclusive and rights-based. In so doing we aim to strengthen

our monitoring, outreach, communication and human rights education, including digital rights literacy.

37. We will work towards strengthening our individual complaints-handling mechanisms and, where necessary and appropriate, explore the responsible and human rights-based use of digital technologies. In doing so, we will aim to ensure that digitalisation enhances accessibility, safeguards privacy and security, and supports effective access to justice and remedies for victims of human rights violations.

38. We will deepen our cooperation through GANHRI and the regional networks to exchange experiences, share information, promote peer learning, strengthen collective capacity and advocate for a responsible and human rights-respecting approach to the development, use and governance of digital technologies.

39. We commit to strengthening GANHRI's collective work on technologies and human rights by supporting a platform for exchange and cooperation among NHRIs on the human rights implications of emerging technologies, including to share experiences, identify good practices, and address common challenges.

40. We call on our partners, including the Office of the United Nations High Commissioner for Human Rights, the United Nations Development Programme, the European Union, regional organizations and other relevant actors, to support us, GANHRI and the regional networks in implementing this statement through sustained technical cooperation, knowledge-sharing and capacity strengthening.

41. As digital transformation advances, we will continue, individually and through GANHRI, to work to ensure that technology remains at the service of people and that its development and use be guided by human rights, accountability and the protection of human dignity.