Policy brief | October 2026
Oxfam in Cambodia | ReCIPE project, co-funded by the European Union

This publication was co-funded by the European Union. Its contents are the sole responsibility of the authors and do not necessarily reflect the views of the European Union.

Protecting people's rights in Cambodia's digital transformation

Introduction

As Cambodia moves more services and activities online, people face barriers to accessing services, risks of harassment and misuse of personal data, and uncertainty about their rights at work. People affected by these changes also need opportunities to influence the laws and policies governing them.

Oxfam in Cambodia commissioned **"Comprehensive Policy Analysis of Cambodia's Digital Transformation"** as part of the Recentering the Civic Internet through Partner Engagement (ReCIPE) project, co-funded by the European Union, to examine these concerns.[1] The research reviewed Cambodia's national laws and policies and compared them with international and regional standards, such as United Nations human rights treaties and Association of Southeast Asian Nations (ASEAN) frameworks. It also included key informant interviews with government officials and policymakers, legal and regulatory experts, United Nations agencies and development partners, private companies, civil society and digital rights organisations. Focus group discussions were organised with rights-holder groups and communities. Based on this evidence, the brief presents recommendations for making digital services accessible, protecting people's rights and strengthening participation in public decisions.

The study used **Oxfam's Rights in a Digital Age (RIADA) framework** to assess how Cambodia's digital transformation affects people's rights. The framework relies on five pillars: **Access and Equity; Security and Digital Civic Space; Responsible Data Use and Privacy; Automation and the Future of Work; and Governance**. The framework was used to examine national laws and policies alongside people's experiences across these five pillars, identify gaps in protection and develop recommendations.

1. Access and Equity: make public services accessible and usable

Access involves more than having an internet connection or a smartphone. People must also be able to understand a service, complete the required steps and obtain assistance.

ACCESS AND EQUITY PRIORITY ACTIONS

Set minimum requirements for government online services

The Ministry of Post and Telecommunications and the Digital Government Committee, chaired by the Minister of Post and Telecommunications, should set minimum requirements that every government online service must meet before it is launched. Each service should work on the phones in common use, be available in Khmer, be usable by people with disabilities, collect only the personal data needed to provide the service, and have staff available to answer users' questions. The draft Law on Digital Government already provides for requirements of this kind to be set.[9]

Test each service before launch

They should also require each service to be tested with the people who will use it before it is released. When the service launches, the date it becomes available and the times when staff can answer questions should be published. The Digital Government Policy already commits to raising public awareness of digital public services, and the draft Law on Digital Government already requires a way for people to give feedback and complain. The research found that people who find a service does not work the first time tend not to try it again.[10]

ACCESS AND EQUITY FURTHER ACTION

Adapt digital literacy training and set targets for the groups reached least

The Ministry of Post and Telecommunications, which owns the national Digital, Media and Information Literacy Competency Framework, should publish practical guidance on using the framework to design digital literacy training, working with the Ministry of Education, Youth and Sport and the Ministry of Labour and Vocational Training. With this guidance, training providers can assess what each group already knows and adapt the content, instead of repeating the same material. The guidance should be freely available to government, civil society and private providers. Delivery targets should be set and published for the groups reached least, including older people, people with disabilities, informal workers and rural communities.[11]

2. Security and Digital Civic Space: protect online safety and freedom of expression

Digital civic space refers to people's ability to discuss public issues, share information and participate in public life online.

SECURITY AND DIGITAL CIVIC SPACE PRIORITY ACTIONS

Make four changes to the draft cybercrime law

The Ministry of Interior, which leads the draft cybercrime law (Draft V.1, unofficial translation), should make four changes as the draft is finalised, working with the Office of the Council of Ministers and the Ministry of Justice:

- Define in the law itself the terms used in Articles 3 and 28, including "sovereignty and integrity", "insecurity", "instability", "moral and cultural values" and "interest of the Kingdom", and state who decides whether content falls within them.
- In Article 28, define what counts as "non-factual" content, require that harm be shown to have occurred, remove imprisonment as a penalty for defamation, and draw the offences narrowly enough that reporting and comment on matters of public interest fall outside them.
- Require a judge's approval for each order to preserve, copy or seize a person's data during an investigation, allow the data to be used only for that investigation, and set a rule on when it is deleted. The Ministry of Post and Telecommunications should take part in this change, because it concerns data held by companies.
- Require a judge's approval for access to a computer system and for the interception of communications, set rules on how intercepted data is stored and when it is deleted, and give the person informed of the measure under Article 20 a way to challenge it. Investigations should stay under the direction of the prosecutor, as the Code of Criminal Procedure provides, rather than under the Secretary General of the National Anti-Cybercrime Committee.

These changes reflect Article 19 of the International Covenant on Civil and Political Rights, an international treaty to which Cambodia is a party and which protects rights including privacy and freedom of expression. They also reflect the safeguards in the Budapest Convention on Cybercrime, which most cybercrime laws follow.[15]

SECURITY AND DIGITAL CIVIC SPACE FURTHER ACTIONS

Extend the police reporting service to online harassment and abuse

The Ministry of Interior, through the Anti-Cybercrime Department of the General Commissariat of National Police, should extend the national police service that receives reports of online scams at any hour, so that it also covers online harassment and abuse. People would then have one official place to report any online harm. Officers who receive these reports should be trained to handle cases where the harm is personal rather than financial, and to receive every report without blame and without regard to the gender identity or sexual orientation of the person reporting.[16]

Raise the moderation of abusive content in Khmer with the companies

The Ministry of Post and Telecommunications, with the Ministry of Interior, should raise with the companies that run the social media and messaging services widely used in Cambodia how they detect and remove abusive content written in Khmer. Abusive terms in Khmer should be treated in the same way as equivalent terms in other languages.

3. Responsible Data Use and Privacy: protect personal and community information

Personal data includes information that identifies someone or can be linked to them. Its collection and use can affect access to services, privacy and safety.

RESPONSIBLE DATA USE AND PRIVACY PRIORITY ACTIONS

Issue guidance on handling personal information now

The Ministry of Post and Telecommunications, which the draft law makes responsible for personal data protection, should issue guidance on how personal information should be handled until the data protection law is adopted and applies. Companies would then know what is expected of them, and people would know what protection to expect. The ASEAN Framework on Personal Data Protection, which Cambodia has endorsed, can serve as its basis.[20]

Give the Personal Data Protection Unit the task of deciding complaints

The draft data protection law allows the government to establish a Personal Data Protection Unit at the request of the Minister of Post and Telecommunications (Article 5). The Ministry should also give this unit the task of deciding complaints from people whose personal data has been misused. This would separate the handling of complaints from the setting and monitoring of the rules, which is the arrangement used in most countries with a data protection law.[21]

Give Indigenous communities a role in decisions on information about them

Digital policies should set out who decides how information about Indigenous communities, their land and their natural resources is held and used, and give those communities a role in that decision. The Ministry of Post and Telecommunications should lead this work, with the Ministry of Rural Development, which issues the letter of recognition for an Indigenous community, and the Ministry of Land Management, Urban Planning and Construction. The Land Law 2001 already recognises an Indigenous community as a body that can hold land collectively, so the same community can be recognised as holding rights over information about that land.[22]

RESPONSIBLE DATA USE AND PRIVACY FURTHER ACTION

Apply data protection rules to ministries and public bodies

The Ministry of Post and Telecommunications, with the Digital Government Committee, should ensure that personal data held by ministries, government institutions and sub-national administrations is covered by rules equivalent to those the draft data protection law sets for companies. The draft law refers to a separate law for the public sector, which does not appear to exist yet. Until it does, people have no stated rights over the information government holds about them. Meanwhile, the national data repository, a central store of government data, and the digital identity system are being built, and the draft Law on Digital Government makes the Committee responsible for both.[23]

4. Automation and the Future of Work: clarify workers' rights and monitor employment changes

Digital platforms connect customers with people providing services, including delivery and ride-hailing. Automation uses technology to perform tasks previously carried out by people. Both can change employment arrangements and working conditions.

AUTOMATION AND THE FUTURE OF WORK PRIORITY ACTIONS

Clarify how the Labour Law applies to people who find work through apps

The Ministry of Labour and Vocational Training should set out how the Labour Law's existing definitions of employer, worker and employment contract apply to people who find work through an app, such as delivery riders and ride-hailing drivers. This can be done without preparing a separate law. Workers would then know which protections apply to them, and the companies that run the apps would know their obligations.

Monitor how digital technology changes work

The Ministry of Labour and Vocational Training and the Ministry of Post and Telecommunications should monitor, on a continuing basis, how digital technology changes work in Cambodia, and publish the findings. This should cover jobs replaced by automation and artificial intelligence, changes in working conditions where technology has been introduced, and the growth of work arranged through apps. The study of effects on jobs planned in the draft National Artificial Intelligence Strategy 2025-2030 (strategic measure 1.9) would give a first picture. Strategic measure 1.9 already asks for special attention to women. Regular monitoring would give government and workers' organisations a shared basis for deciding what support workers need and when.

AUTOMATION AND THE FUTURE OF WORK FURTHER ACTION

Set out how creators can report work copied by artificial intelligence tools

The Ministry of Post and Telecommunications and the National Committee on Intellectual Property Protection should set out how a creative worker whose work, voice or image has been copied by an artificial intelligence tool can report it, and how the report will be considered and answered. The draft National Artificial Intelligence Strategy 2025-2030 already makes these two bodies jointly responsible for respect for intellectual property in the use of artificial intelligence (strategic measure 5.8).[27]

5. Governance: include affected people in decisions and review results

Governance concerns how digital laws and policies are prepared, implemented and reviewed, and how people can influence these decisions.

GOVERNANCE PRIORITY ACTIONS

Publish guidance on consultations and make them easier to attend

The Digital Government Committee, which the Digital Government Policy already asks to consult all stakeholders on digital government plans and projects, should publish guidance on how consultations on digital laws and policies are run, working with the ministries that lead each law or policy. The guidance should set out at what stage a draft is shared, how long people have to respond, and which organisations are invited. It can be introduced without changing an existing policy. Organisations could then plan their input instead of learning of a consultation at short notice.[29]

They should also make consultations easier to attend, for example by holding some sessions outside Phnom Penh or online, covering the travel costs of provincial organisations, and inviting organisations beyond those already known to a ministry and beyond those with technical qualifications.

Assess digital laws for their effect on rights, and review them once in force

The Digital Government Committee, which is responsible for monitoring and evaluating the Digital Government Policy and coordinates the monitoring of the draft artificial intelligence strategy, should ensure, working with the ministries that lead each law or policy, that every draft digital law and policy is assessed for its effect on people's rights before it is adopted, looking at each group separately and at people who belong to several groups at once, and that the assessment is published. Once a law or policy is in force, a working group should review how it is applied at set intervals and publish its findings. The group should include members from outside the ministries applying it: civil society organisations, the private sector and representatives of the groups most affected. The draft Law on Digital Government provides for a sub-decree on the organisation and functioning of the Committee (Article 4), which could establish this group. The draft National Artificial Intelligence Strategy 2025-2030 already commits to risk assessments by sector with the participation of stakeholders (strategic measure 5.5).[30]

GOVERNANCE FURTHER ACTION

Measure how digital laws and policies affect each group

The Digital Government Committee should work with the ministries that lead each law or policy to measure how digital laws and policies affect particular groups, including women, rural communities, older people, people with disabilities and workers. This measurement should sit alongside the current measurement of whether planned actions have been carried out. Results reported by group would show which people a law or service reaches and which it does not, so that it can be adjusted while it is in force rather than at the end of the policy period.[31]

This policy brief was developed as part of the ReCIPE project, co-funded by the European Union, and is based on Oxfam in Cambodia's study, "Comprehensive Policy Analysis of Cambodia's Digital Transformation."

This publication was co-funded by the European Union. Its contents are the sole responsibility of the authors and do not necessarily reflect the views of the European Union.

Notes

1 Oxfam in Cambodia (2026) 'Comprehensive Policy Analysis of Cambodia's Digital Transformation', Phnom Penh: Oxfam in Cambodia.

2 Ibid., section 5.1.

3 Ibid., sections 5.1 and 6.

4 UNESCO (2024) 'Cambodia Launches its First Competency Framework on Digital, Media and Information Literacy to Empower Citizens in Today's Digital Society', 2 July 2024, https://www.unesco.org/en/articles/cambodia-launches-its-first-competency-framework-digital-media-and-information-literacy-empower (last accessed 28 September 2026).

5 Oxfam in Cambodia (2026) op. cit., section 5.1.

6 Ibid., sections 5.1 and 6.1.

7 Draft Law on Digital Government (version dated 21 June 2025), Articles 6(c) and 17. Based on the thirty national digital laws and policies listed in section 4.1 of Oxfam in Cambodia (2026) op. cit.

8 Royal Government of Cambodia (2022) 'Cambodia Digital Government Policy 2022-2035', prepared by the Ministry of Post and Telecommunications, Phnom Penh: Royal Government of Cambodia, section 8.2; Oxfam in Cambodia (2026) op. cit., Annex D.

9 Draft Law on Digital Government, op. cit., Article 17.

10 Royal Government of Cambodia (2022) op. cit.; Draft Law on Digital Government, op. cit., Article 24; Oxfam in Cambodia (2026) op. cit., section 5.5.

11 Ministry of Post and Telecommunications and UNESCO (2024) 'Digital, Media and Information Literacy Competency Framework', 2nd edition, Phnom Penh; Ministry of Post and Telecommunications (2024) 'Roadmap for Digital Skills Development in Cambodia 2024-2035', Phnom Penh: Ministry of Post and Telecommunications, section 4.1.

12 Oxfam in Cambodia (2026) op. cit., section 5.2.

13 Draft Law on Cybercrime, Draft V.1, prepared by the Cybercrime Law Formulation Working Group of the Council of Ministers, unofficial translation, https://data.opendevelopmentcambodia.net/en/laws_record/draft-cybercrime-law (last accessed 28 September 2026), Articles 3, 4 and 28.

14 Ibid., Articles 17, 18 and 20.

15 Ibid., Articles 3, 6, 16, 17, 18, 20 and 28; Oxfam in Cambodia (2026) op. cit., section 4.2 and Annex D.

16 Oxfam in Cambodia (2026) op. cit., Annex D.

17 Ibid., section 5.3.

18 Draft Law on Personal Data Protection (unofficial translation, version dated 31 July 2026), Articles 2 and 57.

19 Land Law 2001, Articles 23 and 26; Draft Law on Personal Data Protection, op. cit., glossary.

20 Draft Law on Personal Data Protection, op. cit., Article 4; Oxfam in Cambodia (2026) op. cit., Annex D.

21 Draft Law on Personal Data Protection, op. cit., Article 5; Oxfam in Cambodia (2026) op. cit., Annex D.

22 Land Law 2001, op. cit., Articles 23 and 26; Oxfam in Cambodia (2026) op. cit., Annex D.

23 Draft Law on Personal Data Protection, op. cit., Articles 2 and 15; Draft Law on Digital Government, op. cit., Articles 11 and 12.

24 Oxfam in Cambodia (2026) op. cit., sections 5.4 and 6.1.

25 Labour Law 1997, as amended in 2007, 2018 and 2021, Articles 1, 2 and 5; Oxfam in Cambodia (2026) op. cit., Annex D.

26 Draft National Artificial Intelligence Strategy 2025-2030 (June 2025), strategic measure 1.9.

27 Ibid., strategic measure 5.8.

28 Oxfam in Cambodia (2026) op. cit., section 5.5.

29 Royal Government of Cambodia (2022) op. cit.

30 Draft Law on Digital Government, op. cit., Article 4; Draft National Artificial Intelligence Strategy 2025-2030, op. cit., strategic measure 5.5 and section V; Royal Government of Cambodia (2022) op. cit., section 8.2.

31 Royal Government of Cambodia (2022) op. cit., section 8.2; Oxfam in Cambodia (2026) op. cit., Annex D.

32 Oxfam in Cambodia (2026) op. cit., sections 3 and 9.1.