Privacy International's Recommendations on Privacy and Data Protection

Revised Fifth Draft Instrument on an International Regulatory Framework on Private Military and Security Companies, OEIGWG — May 2026

Privacy International (PI) is a non-governmental organisation that conducts research and advocates globally against government and corporate abuses of data and technology.[1] It exposes harm and abuses, mobilises allies globally, campaigns with the public for solutions, and pressures companies and governments to change.

Building on our submission prior to the 7th session and reflecting on the emerging debate during the session, PI submits these targeted textual recommendations to strengthen the Revised Fifth Draft Instrument by integrating the right to privacy throughout the text in order to address the growing use of surveillance technologies by PMSCs. When the mandate for the Working Group was established in 2017, surveillance technologies were not featuring significantly in the services provided by PMSCs. Now, as noted by the UN High Commissioner for Human Rights in his opening remarks, PMSCs increasingly engage in surveillance, personal data processing, and the deployment of data-driven technologies are core elements of their operations. Rapid technological advancement has led PMSCs to increasingly prioritise private surveillance, data harvesting, and cyber operations over more traditional security functions.[2] And private companies providing surveillance services for security and/or military purposes are PMSCs.[3]

As noted by many member state delegations and other stakeholders during the 7th session, including the Chair of the UN Working Group on the use mercenaries, the draft instrument should strive to be 'future proof'. However, the current draft does not adequately reflect the current realities of PMSC's reliance on surveillance technologies, leaving a significant regulatory gap that undermines compliance with binding international human rights obligations.

PI's recommendations to fill this gap draw on language which has vast support, including wordings from UN General Assembly and Human Rights Council resolutions adopted by

[1] See: https://privacyinternational.org/about

[2] Ilia Siatitsa, 'Exploring the Privatisation of Surveillance and its Human Rights Implications', *Private Security Considerations: The responsible security forum, ICOCA* (2026), https://blog.icoca.ch/exploring-the-privatisation-of-surveillance-and-its-human-rights-implications/

[3] For an analysis of the typologies of private security companies, see Privacy International and DCAF – Geneva Centre for Security Sector Governance (DCAF), 'Understanding Private Surveillance Providers and Technologies', Policy Paper (2022), https://privacyinternational.org/report/5255/understanding-private-surveillance-providers-and-technologies

consensus.[4] Our recommendations follow the structure of the draft instrument[5] and propose amendments to existing provisions, as well as a small number of new additions — modelled on the instrument's existing approach to weapons regulation — to ensure that privacy and data protection are treated as substantive safeguards rather than mere limitations on transparency.

Summary of Proposed Changes

- **Preamble (new PP6bis)**: Proposed new addition of a stand-alone preambular paragraph recognising privacy and data protection as fundamental rights.
- **Preamble (PP7)**: Proposed amendment to explicitly name surveillance and personal data processing among the activities of concern.
- **Article 1(c)**: Proposed amendment to include surveillance, data collection and processing in the definition of military and security services.
- **Article 5(2)(d)**: Proposed amendment to add data protection impact assessment to due diligence requirements.
- **Article 5(2)(e)**: Proposed amendment to add training on privacy and data protection standards to the training obligation.
- **Article 5(2)(i)**: Proposed amendment to reframe existing privacy reference as a substantive obligation, not just a limitation.
- **New Article 11bis**: Proposed addition of a new provision regulating acquisition and use of surveillance technologies and data systems, modelled on Article 11.

1. Preamble

1.1. New Preambular Paragraph PP6bis — Privacy and Data Protection as Fundamental Rights

The draft instrument does not include any free-standing recognition of privacy and data protection as fundamental rights of relevance to PMSC activities. This is a significant gap because the right to privacy is engaged when PMSCs carry out surveillance as part of their services. Further the UN General Assembly and the UN Human Rights Council have reaffirmed that the right to privacy is one of the foundations of democratic societies and enables the enjoyment of other human rights.[6] A new preambular paragraph, inserted after PP6, would remedy this gap.

[4] For a comprehensive compendium, see Privacy International, Guide to International Law and Surveillance, https://privacyinternational.org/report/5403/pis-guide-international-law-and-surveillance

[5] Revised Fifth Draft Instrument on PMSCs shared on 27 March 2026 revising Fifth Draft Instrument on an international regulatory framework on the regulation, monitoring of and oversight over the activities of private military and security companies released on 1 October 2025 https://www.ohchr.org/en/hr-bodies/hrc/pms-cs/igwg-index/7th-session-igwg-military

[6] UN General Assembly resolution A/RES/79/175, https://digitallibrary.un.org/record/4071978?v=pdf and UN Human Rights Council resolution A/HRC/RES/54/21, https://digitallibrary.un.org/record/4025243?ln=en&v=pdf

This mirrors the structure of existing preambular paragraphs that recall relevant thematic frameworks.

PROPOSED NEW ADDITION
PP6bis *Recalling the right to privacy as guaranteed under Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights, and as elaborated in the UN General Assembly resolutions on the right to privacy in the digital age (A/RES/68/167 and subsequent), as well as applicable regional data protection instruments, and affirming that the collection, processing, storage, and use of personal data by Private Military and Security Companies, their personnel and subcontractors must comply with privacy obligations and with applicable data protection;*
Rationale: PMSCs now routinely collect and process personal data as part of their core operational activities, including through biometric data collection, surveillance systems, intelligence gathering and digital monitoring. The absence of any preambular recognition of privacy and data protection as a foundational framework creates an interpretative gap in the instrument. This addition is modelled on the approach taken in PP4 (IHL) and PP5 (UNGPs) and reflects the growing body of UN guidance on privacy in the digital age.

1.2. Preambular Paragraph PP7 — Concern at Activities of PMSCs

PP7 identifies the risk posed by PMSCs providing services that involve the use of force. It references emerging technologies but does not specifically identify the harm resulting from surveillance, personal data processing or data-driven operations. This creates an implicit exclusion at the level of the preamble, which would be unfortunate given the significant embedding of surveillance technologies in PMSCs services and the human rights abuses directly or indirectly linked to these activities.

Highly intrusive surveillance technologies are now a standard feature of PMSCs operations. Notably biometric surveillance systems — including facial recognition, gait analysis, voice recognition, and behavioural profiling — are increasingly embedded in the operational environments where PMSCs and mercenary actors operate: checkpoints, border crossings, urban surveillance grids, and conflict zones.[7] Companies are equipping themselves with drones fitted with high-resolution cameras and sensors capable of continuous area monitoring, advanced

[7] PI has documented the use of commercial facial recognition systems in border management and post-conflict settings that are often operated by PMSCs and similar contractors. See for example in the UK, Privacy International's response to the UK Home Office consultation on facial recognition technology (5 March 2026) https://privacyinternational.org/advocacy/5741/privacy-internationals-response-uk-home-office-consultation-facial-recognition

facial recognition systems for individual identification and authentication, and a growing array of other high-end surveillance tools. [8]

The spread of these capabilities beyond state actors is already producing documented harms: in the United States, facial recognition technology has been used by private companies to exclude individuals identified as unwanted from public venues; [9] in the United Kingdom, the Facewatch facial recognition network has raised serious concerns about the role of private operators in conducting biometric surveillance of the public without adequate legal basis or oversight.[10] At the early stages of the war in Ukraine, Clearview AI offered its services at the Ukrainian ministry of defense – this is the same company investigated and condemned by multiple data protection authorities around the world for unlawful processing of personal data of millions of people.[11]

Further, the reference to emerging technologies included in the current text would benefit with a clarification of some of the most concerning applications which are already being used by PMSCs, such as artificial intelligence and biometric systems, and which have been singled out in relevant UN resolutions as raising specific human rights concerns.[12]

CURRENT TEXT	PROPOSED AMENDED TEXT
Concerned about the risk posed by excessive or otherwise inappropriate use of Private Military and Security Companies by States for the provision to a variety of clients, of certain services including those involving the use of force, both online and offline, which may be enhanced by the application of emerging technologies and the use of cyberspace, potentially leading to abuses or violations of International Human Rights Law and violations of International Humanitarian Law;	*Concerned about the risk posed by excessive or otherwise inappropriate use of Private Military and Security Companies by States for the provision to a variety of clients, of certain services including those involving the use of force, both online and offline, which may be enhanced by the application of emerging technologies* including surveillance technologies, artificial intelligence and biometric systems, *and the use of cyberspace, potentially leading to abuses or*

[8] Security drones to the rescue in SA, ITWebs (2024) https://www.itweb.co.za/article/security-drones-to-the-rescue-in-sa/P3gQ2qGAg2D7nRD1.

[9] Max Zahn, 'Controversy illuminates rise of facial recognition in private sector', abcNEWS (7 January 2023) https://abcnews.com/Business/controversy-illuminates-rise-facial-recognition-private-sector/story?id=96116545

[10] PI, 'Facewatch: the Reality Behind the Marketing Discourse' (2020) https://privacyinternational.org/long-read/4216/facewatch-reality-behind-marketing-discourse

[11] PI, 'The Clearview/Ukraine partnership - How surveillance companies exploit war' (2022) https://privacyinternational.org/news-analysis/4806/clearviewukraine-partnership-how-surveillance-companies-exploit-war

[12] For example, UN General Assembly resolutions: A/RES/78/213, https://docs.un.org/en/A/RES/78/213; A/RES/79/175, https://digitallibrary.un.org/record/4071978?v=pdf; A/RES/80/58, https://docs.un.org/en/A/RES/80/58

	violations of International Human Rights Law and violations of International Humanitarian Law;

Rationale: Surveillance and data processing are now standard PMSC activities — from border monitoring to intelligence services and crowd management. The UN Working Group on the Use of Mercenaries documented in its 2021 report to the General Assembly that PMSCs may be engaged to conduct malicious cyber operations, exfiltrate information, and conduct surveillance activities that violate the right to privacy, freedom of expression and other fundamental rights, with differentiated impacts on human rights defenders, journalists, and marginalised groups.[13] This amendment ensures that the preamble reflects the contemporary operational reality of the PMSCs industry and places privacy-related concerns on the same footing as other human rights concerns identified in PP7.

2. Article 1(c) — Definition of Military and Security Services

The definition of military and security services in Article 1(c) provides a non-exhaustive list of covered activities. PI welcomes the inclusion of 'intelligence and investigation' in the list. However, surveillance by means of digital technologies is not explicitly listed, despite being significant and growing PMSC activities. This creates interpretative uncertainty as to whether such activities fall within the scope of the instrument.

As noted above. PMSC are increasingly offering surveillance services to their clients, and the technology tools they use or provide go well beyond traditional intelligence methods. They include not only physical surveillance equipment but also the monitoring of digital communications and networks allowing PMSCs broad and largely unchecked access to personal data. The same companies may additionally offer advanced data management and analytics services, enabling the processing of data at a scale and depth that goes well beyond what any defined security purpose would require.[14]

[13] UN Working Group on the Use of Mercenaries, Report to the 76th Session of the UN General Assembly, "Mercenaries, mercenary-related actors and private military and security companies in cyberspace", UN Doc A/76/151, 15 July 2021, https://undocs.org/A/76/151. See also, Méryl Schwitzguébel (DCAF) and Ilia Siatitsa (Privacy International), "When Surveillance Goes Private", Opinio Juris Symposium on PMSCs: The Business of Security, 15 July 2025, https://opiniojuris.org/2025/07/15/symposium-on-pmscs-when-surveillance-goes-private/; Privacy International and DCAF – Geneva Centre for Security Sector Governance, "Understanding Private Surveillance Providers and Technologies", Policy Paper, 2022, https://privacyinternational.org/report/5255/understanding-private-surveillance-providers-and-technologies

[14] PI and DCAF Policy Paper (2022), note above.

CURRENT TEXT	PROPOSED AMENDED TEXT
[…] Military and security services include, in particular, but are not limited to, guarding and protection of persons and objects, such as convoys, buildings and other places; maintenance and operation of weapons systems; prisoner detention; advice to or training of armed and security forces and security personnel; intelligence and investigation; and other logistical and operational support to armed and security forces, whether on land, in the air or at sea, or whether in cyberspace or outer space;	*[…] Military and security services include, in particular, but are not limited to, guarding and protection of persons and objects, such as convoys, buildings and other places; maintenance and operation of weapons systems; prisoner detention; advice to or training of armed and security forces and security personnel; intelligence and investigation, including by means of digital surveillance technologies; and other logistical and operational support to armed and security forces, whether on land, in the air or at sea, or whether in cyberspace or outer space;*
Rationale: The explicit enumeration of surveillance, monitoring, and personal data activities in the definition ensures that these activities are unambiguously within the scope of the instrument. This is consistent with the definitional approach of the Montreux Document, which recognises intelligence and related activities as PMSC services, and reflects current industry practice where data services are often contracted separately from physical security services, potentially allowing them to fall outside narrower definitions.	

3. Article 5 — Obligations with Respect to Registration, Licensing and Recruitment

3.1. Article 5(2)(d) — Human Rights Due Diligence

Article 5(2)(d) requires PMSCs to undertake human rights due diligence including human rights and environmental impact assessments. A data protection impact assessment (DPIA) should be explicitly included within the due diligence framework.

As noted by the UN High Commissioner for Human Rights "in an increasingly complex technological environment, [privacy impact] assessments assume a key role in preventing and mitigating privacy harms companies" and "must provide for adequate processes and safeguards to prevent and mitigate potential privacy and other human rights harms".[15]

[15] A/HRC/39/29, paras 31 and 46.

In this context, DPIA is a requirement that has been integrated into national data protection regional standards and domestic laws, including in Article 10 of the Council of Europe Convention for the protection of individuals with regard to the processing of personal data,[16] Article 35 of the EU General Data Protection Regulation.[17] It requires an impact assessments prior to processing personal data, particularly where the data processing may result in risk to the rights and freedoms of individuals, such as when the processing involves sensitive personal data, automated decision-making, profiling, or monitoring of public spaces, all activities often performed by PMSCs.

CURRENT TEXT	PROPOSED AMENDED TEXT[18]
promote the undertaking of human rights due diligence and human rights impact assessment to identify, prevent and mitigate the risks of negative human rights impacts and abuses arising from their activities which will include human rights, gender equality, labour and environmental impact assessments prior and throughout their operations;	*promote the undertaking of human rights due diligence, including human rights impact assessment to identify, prevent and mitigate the risks of negative human rights impacts and abuses arising from their activities, which will include human rights, gender equality, labour, environmental and data protection impact assessments prior and throughout their operations;*
Rationale: Data protection impact assessments are a well-established tool in international and regional practice for identifying and mitigating privacy risks before systems are deployed. Requiring PMSCs to conduct DPIAs as part of their due diligence obligations is consistent with the instrument's existing due diligence framework and with the UNGPs, which the OHCHR has confirmed apply to technology and data-related activities of private actors (A/HRC/59/32, June 2025).	

3.2. Article 5(2)(e) — Training Obligations

Article 5(2)(e) sets out training requirements for PMSC personnel. It currently covers IHL, IHRL, gender equality, use of force, and related subjects. Training on privacy law and data protection standards could be added explicitly, given that personnel routinely handle personal data, conduct surveillance, and operate data systems.

[16] Council of Europe, Convention 108 +, Convention for the protection of individuals with regard to the processing of personal data, https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1

[17] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

[18] Please note that this edit is not reflected in the joint proposal with other civil society organisations. It is an alternative edit, if the joint alternative proposal is not accepted.

PMSC personnel are often handling sensitive personal information as part of the performance of their services, most notably in relation to surveillance, intelligence gathering and monitoring of communications networks. Failing to know and to apply data protection principles, such as those related to cybersecurity measures, steps against unauthorized access and process of to address and notify data breaches, can have significant negative consequences on the individuals whose personal data pertained to.

CURRENT TEXT	PROPOSED AMENDED TEXT
promote training in International Human Rights Law and International Humanitarian Law, gender equality principles and standards, and relevant standards (domestic law) and rules governing the individual use of force,[34] guided by the personal right of self-defence and the defence of others and, where applicable, the purchase, marking, storage, use and management of weapons and ammunition, the protection of the environment, the use of lethal and non-lethal equipment and the prevention of labour and sexual exploitation and abuse, including in situations of armed conflict;	*conduct training in International Human Rights Law and International Humanitarian Law, gender equality principles and standards, and relevant standards (domestic law) and rules governing the individual use of force,[34] guided by the personal right of self-defence and the defence of others and, where applicable, the purchase, marking, storage, use and management of weapons and ammunition, the protection of the environment, the use of lethal and non-lethal equipment, the lawful use of surveillance technologies and the responsible handling of personal data, and the prevention of labour and sexual exploitation and abuse, including in situations of armed conflict;*
Rationale: Privacy and data protection training is a core element of responsible PMSCs operations in the digital age. This amendment ensures alignment between the instrument's training obligations and the substantive standards proposed elsewhere in these recommendations. It also reflects the approach of the ICoC, which requires security companies to train personnel on applicable legal frameworks, and of the UNGPs.	

3.3. Article 5(2)(i) — Transparency and Privacy

Article 5(2)(i) currently mentions personal privacy (together with commercial confidentiality) only as limitations on the obligation of contract transparency. This inadvertently frames privacy as a constraint on accountability rather than as a substantive right that PMSCs must respect in their data handling practices. The provision should be restructured to reflect this distinction.

As noted above, the processing of personal data is often a key component of PMSCs services. As such, they should implement technical and organisational measures to ensure their processing of personal data is compliant with modern data protection standards and domestic laws.[19]

[19] See for example Article 10(3) of the Council of Europe, Convention 108 +, Convention for the protection of individuals with regard to the processing of personal data, https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1; and Article 24 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of

However, this is often not the case in practice and including it in Article 5, which lists the policies that PMSCs should adopt and implement to qualify for a licence, would be an effective means to bring PMSCs activities in line with data protection standards.

In terms of data protection principles, there is a growing global consensus on minimum standards that should govern the processing of personal data by States, business enterprises and other private actors, as noted by the UN High Commissioner for Human Rights, including that personal data processing should be necessary and proportionate to a legitimate purpose and that change of purposes should be limited to purposes compatible with the initially specified purpose.[20]

CURRENT TEXT	PROPOSED AMENDED TEXT
promote transparency of contracts for the provision of military and security services by contractors and sub-contractors and adequate transparency of the beneficial ownership status of such contractors and sub-contractors, with respect to the appropriate authorities; [subject to legitimate requirements of personal privacy and commercial confidentiality];	*promote transparency of contracts for the provision of military and security services by contractors and sub-contractors and adequate transparency of the beneficial ownership status of such contractors and sub-contractors, with respect to the appropriate authorities; [subject to legitimate requirements of personal privacy and commercial confidentiality]; and ensure that in the performance of their services, Private Military and Security Companies, their personnel and subcontractors process personal data in accordance with data protection principles;*
Rationale: The current formulation treats privacy only as a qualification on the transparency obligation, creating a misleading impression that privacy interests are in tension with accountability. This addition rebalances the provision by placing a positive obligation on PMSCs to comply with data protection principles in their operations. This is consistent with the UNGPs' Pillar II expectations on respect for human rights.	

4. New Article 11bis — Regulation of Surveillance Technologies and Data Systems

The most significant gap in the current draft is the absence of any provision governing the acquisition and use of surveillance technologies and data systems by PMSCs. Article 11 provides a detailed framework for regulating the acquisition and use of conventional weapons. PI recommends the insertion of a parallel article — Article 11bis — modelled on that structure, to address the analogous risks posed by surveillance and data technologies.

personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

[20] A/HRC/39/29, para 29.

The need to regulate the use, sale and transfer of surveillance technologies stem from states' obligation to respect and protect the right to privacy and other human rights under legally binding international treaties, such as the ICCPR. Numerous resolutions by the UN General Assembly and the Human Rights Council, adopted by consensus, have confirmed this obligation and specifically called on states, inter alia, to:

- review their procedures, practices and legislation regarding the surveillance, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law;
- establish or maintain existing independent, effective, adequately resourced and impartial judicial, administrative and/or parliamentary domestic oversight mechanisms;
- provide individuals whose right to privacy has been violated by unlawful or arbitrary surveillance with access to an effective remedy, consistent with international human rights obligations.[21]

When it comes to the regulation of the sale, export and transfer of surveillance technologies, human rights experts have long advocated for stringent controls (and bans) to prevent these technologies ending up at the disposal of state or non-state actors, including PMSCs, with poor records of human rights. For example, already in 2021 UN special procedures called for the establishment of a moratorium on the sale and transfer of surveillance technology until they have put in place robust regulations that guarantee its use in compliance with international human rights standards, given the documented grave human rights abuses committed.[22]

Indeed this is not a hypothetical risk: PI and other organisations have documented numerous examples of transfer of surveillance technologies resulting in grave human rights abuses, including leading to arbitrary detention and torture.[23] A significant development is the entry into force of the EU export control rules which will make human rights issues a central consideration for export control authorities when assessing licenses and require them to publish data on their decisions to hold them accountable.[24]

In a clear acknowledgment of the significant links between surveillance and use of force the Human Rights Council, in its Resolution on the Promotion and protection of human rights in the context of peaceful protests called "*upon* States to refrain […] from the export, sale or transfer

[21] See for example UN General Assembly resolution A/RES/79/175. For additional references see Privacy International's Guide to International Law and Surveillance, May 2024.

[22] OHCHR, 'Spyware scandal: UN experts call for moratorium on sale of 'life threatening' surveillance tech', 2021, https://www.ohchr.org/en/press-releases/2021/08/spyware-scandal-un-experts-call-moratorium-sale-life-threatening

[23] For some examples, see Privacy International, Surveillance Industry Finally Facing Scrutiny, but Will it Change Anything? https://www.privacyinternational.org/explainer/4720/surveillance-industry-finally-facing-scrutiny-will-it-change-anything

[24] HRW, PI and others, 'Human Rights Organisations' Response to the Adoption of the New EU Dual Use Export Control Rules', https://www.hrw.org/sites/default/files/media_2021/03/Reforms%20to%20EU%20Surveillance%20Tech%20Export%20Rules_Joint%20NGO%20Statement_20210324_0.pdf

of surveillance goods and technologies and less-lethal weapons when they assess that there are reasonable grounds to suspect that such goods, technologies or weapons might be used to violate or abuse human rights, including in the context of assemblies".[25]

For all the above reasons PI recommends the inclusion of this new article in the draft instrument.

PROPOSED NEW ADDITION
ARTICLE 11bis REGULATION OF THE ACQUISITION AND USE OF SURVEILLANCE TECHNOLOGIES AND DATA SYSTEMS *(1) States Parties and States Participants shall adopt or strengthen in their domestic law appropriate measures to:* *(a) regulate and apply effective oversight and control over the acquisition and use of surveillance technologies, including biometric systems, artificial intelligence-based tools and other technologies, by Private Military and Security Companies, their personnel and sub-contractors, in accordance with applicable international human rights law;* *(b) prohibit any transfer to and use by Private Military and Security Companies, their personnel or subcontractors, of surveillance technologies or data systems the design or foreseeable use of which is incompatible with international human rights law;* *(c) prohibit Private Military and Security Companies, their personnel and subcontractors from the unlawful processing, transfer, or sale of personal data processed in the course of their operations.* *(2) This provision does not prejudice the applicability of international instruments, regional frameworks or domestic laws governing data protection, cybersecurity or the use of surveillance technologies.*
Rationale: The regulation of surveillance technologies is among the most significant gaps in the current draft. PMSCs are increasingly deployed to conduct surveillance operations, manage biometric databases, and operate AI-based monitoring systems, including in conflict zones and in migration management contexts. These activities have well-documented human rights impacts, including on the rights to privacy, freedom of expression, freedom of assembly, and non-discrimination. Article 11 already establishes a detailed framework for regulating weapons — technologies with comparable potential for human rights harm. The absence of a parallel provision for surveillance and data technologies is inconsistent with the instrument's overall architecture. This proposed Article 11bis is closely modelled on Article 11 in structure and drafting style, ensuring consistency with the existing text. The provision draws on the framework established in the Council of Europe Convention 108+, the UN General Assembly resolutions on the right to privacy in the digital age, and the OHCHR guidance on privacy and surveillance (A/HRC/27/37, June 2014).

[25] A/HRC/RES/50/21 (8 July 2022).