Submission to Commerce and Economic Development Bureau
On the Consultation of Real-name Registration Programme for SIM Cards

Amnesty International Hong Kong
19 March 2021

A. Introduction

1. The Communications and Creative Industries Branch of the Commerce and Economic Development Bureau (CEDB) issued the consultation paper to seek the views on a proposed real-name registration programme for subscriber identity module (SIM) cards.

2. **The real-name registration programme for SIM card ("SIM card registration") undermines the right to privacy.** It involves mass monitoring, interception, collection, storage, or other use of communications material, that is not targeted at an individual, a particular group or location, and will make it harder to communicate anonymously – a crucial enabler of the right to privacy. Thus, Amnesty International Hong Kong (AIHK) believes that this proposal is not a proportionate and necessary interference and may violate the right to privacy.

3. **The SIM card registration hampers the right to freedom of expression.** With the enactment of the National Security Law (NSL), it allows law enforcement agencies (LEA) additional investigative powers, while bypassing oversight by Hong Kong's legislative and judicial system. AIHK fears that such authorities may multiple the risk induced by the registration SIM-card registration, as the access to the personal data can be given to the authorities without adequate oversight mechanism, which may interfere the right to freedom of peaceful assembly, association and expression in the foreseeable future.

Recommendation

4. AIHK would hereby express grave concern on the impacts on human rights arising from the SIM-card registration programme. This programme does not constitute a justifiable interference with the rights to privacy and freedom of expression. **AIHK therefore urges the Government to scrutinise the consequences of this programme and ensure all measures implemented by the programme must be necessary and proportionate under international human rights law and contain sufficient safeguards against human rights abuse.**

B. An intervention in the rights to privacy

5. Rights to one's privacy is safeguarded by international human rights law, as stated in the Article 17 of International Covenant on Civil and Political Rights, 'No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation', and 'Everyone has the right to the protection of the law against such interference or attacks.'[1]

6. SIM card registration is a form of interference with an individual's right to privacy. According to the report to the Office of the United Nations High Commissioner for Human Rights 'The Right to

[1] Article 17 of the International Covenant on Civil and Political Rights

香港九龍渡船街 32-36 號富利來商業大廈 3 樓 D 室
Unit 3D, Best-O-Best Commercial Centre, 32-36 Ferry Street, Kowloon, Hong Kong
T: +852 2300-1250 E: admin-hk@amnesty.org.hk
F: +852 2782-0583 W: http://www.amnesty.org.hk

Privacy in the Digital Age' (Digital Age Report)[2], there are three overarching principles to determine whether such interference is unlawful or arbitrary: legality, necessity and proportionality:

6.1. Legality: 'Any limitation to privacy rights … must be provided for by law, and the law must be sufficiently accessible, clear and precise so that an individual may look to the law and ascertain who is authorized to conduct data surveillance and under what circumstances';
6.2. Necessity: 'The limitation must be necessary for reaching a legitimate aim'; and
6.3. Proportionate: 'in proportion to the aim and the least intrusive option available amongst those which might achieve the desired result'.

7. The legal basis of SIM card registration should not only come from the national law, i.e. the Basic Law and National Security Law in Hong Kong, but also comply with the International covenant**.** As the Human Rights Committee indicates on the term 'unlawful' that, 'Interference authorized by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives of the Covenant'[3]. Therefore, as the Digital Age Report stated, 'interference that is permissible under national law may nonetheless be "unlawful" if that national law is in conflict with the provisions of the International Covenant on Civil and Political Rights'[4].

8. As a result, even if SIM card registration is on the grounds of national security or prevention of crimes does not make such a policy legitimate. 'The degree of interference must be assessed against the necessity of the measure to achieve that aim and the actual benefits it yields towards such purposes'[5]. For the assessment of the necessity, 'the Human Rights Committee, in its general comment No. 27, on article 12 of the International Covenant on Civil and Political Rights, stressed that "the restrictions must not impair the essence of the right". The Committee further explained that "it is not sufficient that the restrictions serve the permissible purposes; they must also be necessary to protect them." Therefore, 'mass or "bulk" surveillance programmes may thus be deemed to be arbitrary, even if they serve a legitimate aim and have been adopted on the basis of an accessible legal regime'[6].

Recommendation

9. Since SIM card registration is an indiscriminate collection of personal data from all mobile users in Hong Kong, **AIHK urges the government to ensure that the implementation should comply with international human rights law, including the right to privacy. There should be a 'clear, precise, accessible, comprehensive and non-discriminatory legislative framework' and 'effective, independent and impartial oversight'[7] mechanism to guarantee such.**

C. Right to stay anonymous as a gateway for freedom of expression

10. The right to stay anonymous is crucial to ensure one's right to freedom of expression and opinions is well protected. As stated in the Report of the Special Rapporteur on the promotion and protection

[2] Report to the Office of the United Nations High Commissioner on Human Rights, The Right to Privacy in the Digital Age, UN Doc. A/HRC/27/37, para. 21
[3] Official Records of the General Assembly, Forty-third Session, UN Doc. Supplement No. 40 (A/43/40), annex VI, para. 3
[4] Report to the Office of the United Nations High Commissioner on Human Rights, The Right to Privacy in the Digital Age, UN Doc. A/HRC/27/37, para. 21
[5] Report to the Office of the United Nations High Commissioner on Human Rights, The Right to Privacy in the Digital Age, UN Doc. A/HRC/27/37, para. 24
[6] Report to the Office of the United Nations High Commissioner on Human Rights, The Right to Privacy in the Digital Age, UN Doc. A/HRC/27/37, para. 25
[7] Report to the Office of the United Nations High Commissioner on Human Rights, The Right to Privacy in the Digital Age, UN Doc. A/HRC/27/37, para. 50 & 51

of the right to freedom of opinion and expression by David Kaye (David Kaye Report), privacy is 'the gateway for freedom of opinion and expression', and 'Encryption and anonymity provide individuals and groups with a zone of privacy online to hold opinions and exercise freedom of expression without arbitrary and unlawful interference or attacks.' [8]

11. The David Kaye Report concluded that at para 56 in that, 'restrictions on encryption and anonymity must be strictly limited according to principles of legality, necessity, proportionality and legitimacy in objective.'[9] However, as indicated at para 51, 'Compulsory SIM card registration may provide Governments with the capacity to monitor individuals and journalists well beyond any legitimate government interest.'[10] SIM card registration undermines the ability of users to communicate anonymously and one's right to privacy. This poses a threat to vulnerable groups and facilitates surveillance by making tracking and monitoring of users easier for law enforcement authorities.[11]

12. Therefore, as suggested in the David Kaye Report that 'States should not restrict encryption and anonymity, which facilitate and often enable the rights to freedom of opinion and expression', and 'should refrain from making the identification of users a condition for access to digital communications and online services and requiring SIM card registration for mobile users'.[12]

13. In another report on freedom of expression on privacy and communications surveillance, United National Special Rapporteur Frank La Rue (Frank La Rue Report), stressed that restrictions on anonymity will make individuals more vulnerable to state surveillance. Meanwhile, restrictions will have a chilling effect that undermine individuals' rights to expression and information and exacerbating social inequalities.[13]

Recommendation

14. As the right to encryption and anonymity are interlinked and mutually dependent with freedom of expression, **AIHK calls on the government not to adopt any restriction on anonymity unless all restrictive measures meet the requirements of necessity and proportionality under international human rights law. The rights to freedom of expression should be put at the utmost priority**, as any form of surveillance should be regarded as a highly intrusive act that potentially interferes with such. Meanwhile, all restrictions on anonymity must be the least intrusive measures available to achieve the desired legitimate aim.

D. Legal Void

15. The implementation of SIM card registration is backed up by the Personal Data (Privacy) Ordinance. According to the Consultation paper, 'The storage and use of the personal particulars will also need to comply with the relevant requirements including the Data Protection Principles under the Personal Data (Privacy) Ordinance (Cap. 486), e.g. on data security, access, sharing and correction,

[8] Report to the Human Right Council, Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, UN Doc. A/HRC/29/32 (2015), para. 16
[9] Report to the Human Right Council, Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, UN Doc. A/HRC/29/32 (2015), para. 56
[10] Report to the Human Right Council, Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, UN Doc. A/HRC/29/32 (2015), para. 51
[11] Privacy International, *SIM Card Registration*, https://privacyinternational.org/learn/sim-card-registration
[12] Report to the Human Right Council, Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, UN Doc. A/HRC/29/32 (2015), para. 60
[13] Report to the Human Right Council, Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, UN Doc. A/HRC/23/40 (2013), para. 49

etc.'[14] According to GSMA, 59% of countries implementing mandatory SIM card registration are with privacy protection framework.'[15] AIHK is concerned about if Personal Data (Privacy) Ordinance (PDPO) is secure enough to protect the personal data from privacy infringement. Comparing PDPO with General Data Protection Regulation (GDPR), the protection framework of European Union (EU), the protection of personal data in Hong Kong is less comprehensive in the following areas:

15.1. In terms of sensitive personal data, in GDPR, sensitive data has been clearly defined, including
    15.1.1. personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs;
    15.1.2. trade-union membership;
    15.1.3. genetic data, biometric data processed solely to identify a human being;
    15.1.4. health-related data;
    15.1.5. data concerning a person's sex life or sexual orientation.[16]

    The data above is subject to specific processing conditions, as listed in Art 4, 9 and Recital 51 to 56 under GDPR; however, "there is no distinction between sensitive and non-sensitive personal data for all purposes"[17] in PDPO.

15.2. In terms of consent of collection of personal data, as stated in the Recital 32 of GDPR, 'Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them.'[18] Also, GDPR clearly defined consent, stated in Article 4(11), as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."[19] On the other hand, for PDPO, consent is not a pre-requisite for the collection of personal data, unless the personal data is used for a new purpose [Data Protection Principles (DPP) 1&3];[20] for other purposes, where consent is also required, consent only means express and voluntary consent.[21]

15.3. For enhanced rights for data subjects to take control over their personal data collected by the data processors, there is a more comprehensive protection in GDPR. The data subjects can enjoy:

    15.3.1. rights to erasure (to be forgotten) [Art. 17] — Rights for individuals to have their personal data erased;
    15.3.2. restriction of processing [Art. 18] — Rights for individuals to request the restriction or suppression of the use of their personal data, i.e., the personal data is permitted to store, but not to use it;
    15.3.3. data portability [Art. 20] — Rights for individuals to obtain and reuse their personal data for their own purposes across different services; and

---

[14] HKSAR Government, *Real-name Registration Programme for SIM Cards Consultation Paper*, 2021, para. 3(9)
[15] GSMA, *Access To Mobile Services And Proof Of Identity 2020: The Undisputed Linkages*, 2020
[16] European Commission, *What personal data is considered sensitive?,* 2020, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en
[17] Hong Kong Lawyer, *EU GDPR and HK PDPO: What's the Difference?,* 2018, http://www.hk-lawyer.org/content/eu-gdpr-and-hk-pdpo-what%E2%80%99s-difference
[18] Recital 32 of the General Data Protection Regulation (EU) 2016/679
[19] GDPR.EU, *What are the GDPR consent requirements?*, https://gdpr.eu/gdpr-consent-requirements/
[20] Schedule 1, Data Protection Principles 1 and 3 of Personal Data (Privacy) Ordinance Cap. 486
[21] Hong Kong Lawyer, *EU GDPR and HK PDPO: What's the Difference?,* 2018, http://www.hk-lawyer.org/content/eu-gdpr-and-hk-pdpo-what%E2%80%99s-difference

15.3.4. object of processing (including profiling) [Art 21] — Rights for individuals to object to the processing of their personal data in certain circumstances.[22]

However, in PDPO, there is no guaranteed rights of above for data subjects, even though they can make data access and correction requests [DPP6, Part 5] and opt out from direct marketing activities [ss.35G &35L].[23]

16. For the responsibilities of data processors, the consultation paper listed out telecommunication operators' (licensee) duties including to 'check, clarify and verify the information provided by users, and to deregister the concerned SIM cards if there is reasonable ground to believe that the information provided is false, misleading or incomplete.' The consultation paper also stated that 'the personal information of the registered SIM card users should be kept and stored… for at least 12 months after the SIM cards are deregistered.'[24]

16.1. This enables the licensee to collect and store vast sum of personal data for a considerable amount of time, even if the customers no longer use the service. The verification process may also legitimate them to collect extra sensitive information from the customers. The outsource of responsibilities to licensees increases the risk of abusive use of personal data and potential information breach.

16.2. In addition, in terms of accountability and governance, the accountability principle and the related privacy management measures for data controllers are not explicitly stated in PDPO. Also, the data processors are not directly regulated by PDPO [s.2 (12)].[25] In GDPR, however, data processors are obliged to maintain records of processing, ensure security of processing, report data breaches, designate Data Protection Officers, etc. [Art 30, 32-33, 37]; on the other hand, data controllers are required to implement technical and organisational measures to ensure compliance; to adopt data protection by design and by default; to conduct data protection impact assessment for high-risk processing; and (for certain types of organisations) to designate Data Protection Officers [Art 24, 25, 35 and 37],[26] in order to ensure and to be able to demonstrate that processing is performed in accordance with GDPR.

17. As for the responsibilities of licensees, the David Kaye Report suggested at para 62, 'corporate actors should review the adequacy of their practices with regard to human right norms.' 'Companies… should refrain from blocking or limiting the transmission of encrypted communications and permit anonymous communication. Corporate actors that supply technology to undermine encryption and anonymity should be especially transparent as to their products and customers.'[27]

Recommendation

18. AIHK urges the government to review the legal framework of PDPO before implementing the SIM card registration in the following areas:

---

[22] Article 17, 18, 20 and 21of the General Data Protection Regulation (EU) 2016/679
[23] Hong Kong Lawyer, *EU GDPR and HK PDPO: What's the Difference?,* 2018, http://www.hk-lawyer.org/content/eu-gdpr-and-hk-pdpo-what%E2%80%99s-difference
[24] HKSAR Government, *Real-name Registration Programme for SIM Cards Consultation Paper*, 2021, para. 3(9) & 3(10)
[25] Hong Kong Lawyer, *EU GDPR and HK PDPO: What's the Difference?,* 2018, http://www.hk-lawyer.org/content/eu-gdpr-and-hk-pdpo-what%E2%80%99s-difference
[26] Hong Kong Lawyer, *EU GDPR and HK PDPO: What's the Difference?,* 2018, http://www.hk-lawyer.org/content/eu-gdpr-and-hk-pdpo-what%E2%80%99s-difference
[27] Report to the Human Right Council, Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, UN Doc. A/HRC/29/32 (2015), para. 62

18.1. **A more definite distinction between sensitive and non-sensitive data should be drawn**, so that data in different categories are subject to specific processing conditions;

18.2. **For the consent of use of data, it should cover all processing activities carried out for all purposes, not just for transferring to the third parties or other new purposes**, but also including collection; and consent should be specific, informed and unambiguous indication of the will of data subject and given without additional conditions, instead of just express and voluntary consent;

18.3. **PDPO should adopt enhanced rights for data subjects to take control over their personal data collected by the data processors**, so that the data subjects can enjoy rights to erasure (to be forgotten, restriction of processing, restriction of data portability and object of processing (including profiling);

18.4. **In terms of accountability and governance, mandatory requirements should be made for the data controllers (or licensees) to protect the data collected, and to have a holistic mechanism to ensure the process of handling data is in accordance with PDPO**;

18.5. **All measures that are intended to restrict anonymity must be overseen by an effective, impartial and independent civilian oversight authority so as to ensure the processing of personal data are in compliance with the PDPO**.

19. **AIHK urges the telecommunication operators who possess the personal data adopt a more refined data storage system with better encryption and implement a thorough, robust and transparent human rights due diligence (HRDD) process to identify, present and address human rights abuses and ensure the rights to privacy and freedom of expression**.

E. The power of LEA or relating authorities to request for information from licensees

20. As stated in the Consultation Paper, 'LEAs can request licensees to provide SIM cards registration records pursuant to a warrant issued by a magistrate.' However, the consultation paper added that 'relevant LEAs could …request licensees to urgently provide registration information of a SIM card user under exceptional circumstances to deal with certain urgent or emergency situations' when:

20.1. 'considering the nature of certain crimes (e.g., homemade bombs, kidnapping, drug trafficking and smuggling, etc.) that necessitates swift enforcement actions to be taken';
20.2. 'where the application for a magistrate warrant would cause undue delay resulting in loss or destruction of evidence';
20.3. 'there is reasonable ground for suspecting that a serious offence has been, is being, or is about to be committed that it is necessary to obtain the registration information … for investigation or prevention of the offence', and;
20.4. 'for any reason it is not reasonably practicable to make the application'[28].

The government listed out situations where LEA could request for the registration information of a SIM card user without a warrant issued by the magistrate. However, for the nature of certain crimes and serious offences, the government only provided a few examples without specifying a prescribed and comprehensive list of criminal offenses which necessitates swift enforcement actions to be taken. Overshadowed by the enactment of national security law, LEA may arbitrarily extend its scope so as to facilitate surveillance and pose a threat to vulnerable groups.

[28] HKSAR Government, *Real-name Registration Programme for SIM Cards Consultation Paper*, 2021, para. 3(14)

21. The fact the SIM card registration programme is backed up by the National Security Law does not mean it is lawful or legitimate for the LEA to extend its scope of surveillance. As the report of the Office of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age stated, 'neither do laws or rules that give the executive authorities, such as security and intelligence services, excessive discretion; the scope and manner of exercise of authoritative discretion granted must be indicated (in the law itself, or in binding, published guidelines) with reasonable clarity. A law that is accessible, but that does not have foreseeable effects, will not be adequate'[29].

22. The Press Release by the government also stated that 'Under the regulation, LEAs could only request the registration information of a SIM card (i.e. the name and basic identity document information), but not call records and other contents.'[30] However, in the Press Conference, the spokesman did not rule out such regulation will expand to collect further information, e.g., incorporating biometric data, such as fingerprints and facial recognition data. This may also apply to the records of communications, including text messages and verbal conversations.

Recommendation

23. As mentioned, **AIHK maintains that all restrictions on anonymity must be the least intrusive measures available to achieve the desired legitimate aim.** Meanwhile, the government must ensure that all restrictions and intrusions on anonymity authorized by the law:

    23.1. are publicly accessible;
    23.2. contain provisions that ensure that collection of, access to, and use of communications data are tailored to specific legitimate aims;
    23.3. are sufficiently precise, specifying in detail the precise circumstances in which any such interference may be permitted, the procedures for authorizing, the categories of persons who may be placed under surveillance, the limits on the duration of surveillance, and procedures for the use and storage of the data collected; and provide for effective safeguards against abuse[31].

24. In addition, the implementation of SIM card registration programme has to be transparent, precise and legitimate. There should be effective safeguards against the abusive power of collecting the data, and no secret implementation should be adopted. The SIM card registration programme must not be used to target whistle blowers or other individuals seeking to expose human rights violations, nor should they hamper the legitimate oversight of government action by citizens. Court-ordered decryption, subject to domestic and international law, may only be permissible when it results from transparent and publicly accessible laws applied solely on a targeted, case-by-case basis to individuals (i.e., not to a mass of people) and subject to judicial warrant and the protection of due process rights of individuals.'[32] **Thus, AIHK believes the SIM card registration programme requires stronger safeguards in confining LEA's authorities to acquire SIM card registration records from licensees. AIHK proposes that LEA can only request for the registration information of a SIM card user under a warrant issued by the magistrate or above without any exceptional circumstance.**

---

[29] Report to the Office of the United Nations High Commissioner on Human Rights, The Right to Privacy in the Digital Age, UN Doc. A/HRC/27/37, para. 29
[30] HKSAR Press Release, *Public views sought on Real-name Registration Programme for SIM Cards*, 2021 https://www.info.gov.hk/gia/general/202101/29/P2021012900421.htm
[31] Report to the Office of the United Nations High Commissioner on Human Rights, The Right to Privacy in the Digital Age, UN Doc. A/HRC/27/37, para. 28
[32] Report to the Human Right Council, Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, UN Doc. A/HRC/29/32 (2015), para. 60

25. The monitoring of the process of LEA requesting for data from licensees should be independent. **The oversight of surveillance programme should involve 'all branches of government' as well as 'an independent civilian oversight agency', to ensure the effective protection of law.**[33]

F. Discrimination and exclusion

26. The consultation paper stated that 'Registration of an SSP or PPS user below the age of 16 (young person) should be endorsed by an "appropriate adult" who may be the parent, relative or guardian of the young person'. This implies that a person below 16 years old could not register their own personal SIM card on behalf of themselves.

27. SIM registration also brings the potential for discrimination and even exclusion from basic services for the most marginalised groups, like asylum seekers and those who're not able to produce any valid identity documents. This can have a discriminatory effect by excluding users from accessing mobile networks eventually resulting in exclusion from numerous vital public services.

28. In addition, given the extra burdens that SIM registration places on the telecommunication operators, this may result in additional costs being passed on to customers, making grassroots more vulnerable and creating digital gap.

Recommendation

29. SIM card registration can have a disproportionate impact on marginalized groups, undermining the right to equality and non-discrimination, especially on asylum seekers and teenagers under 16. Exclusion from readily access to mobile network of a particular group of people, are nonetheless a risk that can exacerbate and entrench existing social disadvantages and further disempower already-marginalized groups of people. The government should not disregard the rights of these people in the digital world.

30. Therefore, **AIHK urges the government to consider that all measures intended to restrict anonymity must not be discriminatory against specific individuals or groups on the basis of race, sex/gender, sexual orientation, gender identity, religion or belief, political or other opinion, ethnicity, national or social origin, disability, or other status.**

G. Conclusions

31. As a result of these observations, AIHK submits that the current provision of the SIM card registration is a mass violation, which is neither necessary nor proportionate, of international human rights law and standards on the rights to privacy and rights to stay anonymous due to the bulk information collected and the not well-developed POPD. This provision also poses a substantial risk of breaching the human rights to freedom of expressions due to the expansion of power of LEAs and the enactment of NSL. Finally, it potentially undermines the right to equality and non-discrimination, such as refugees' and children's rights.

32. AIHK therefore urges the Hong Kong Government to stop implementing the present proposed SIM card registration until sufficient human rights safeguards that are in line with international human

[33] Report to the Office of the United Nations High Commissioner on Human Rights, The Right to Privacy in the Digital Age, UN Doc. A/HRC/27/37, para. 37

rights laws and standards are in place. **AIHK calls on the government to revise the provision of SIM card registration, as well as the Personal Data (Privacy) Ordinance, so that these surveillance measures comply with the following principles and will not become an arbitrary and unlawful intrusion to the basic human rights:**

32.1. Legality: should be prescribed by not just the national law but also international human laws, meeting a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of and can foresee their application; no executive authorities, such as security and intelligence services, are given excessive discretion and the scope and manner of discretion granted must be with reasonable clarity;

32.2. Necessity: should only be adopted when strictly and demonstrably necessary to achieve a legitimate aim, and the rights to privacy and to freedom of expression should be put at the utmost priority; must not be used to target whistle-blowers or other individuals seeking to expose human rights violations;

32.3. Proportionality: must be the least intrusive measures available to achieve the desired legitimate aim, and should not be employed when less invasive techniques are available or have not yet been exhausted;

32.4. Effective Oversight: the oversight of the programme should involve 'all branches of government' and 'an independent civilian oversight agency', to ensure effective protection of law, and also to ensure the programme complies with international human rights laws; apply sufficient safeguards to prevent the abuse LEA's authorities; and the legal framework (like PDPO) should be revised to ensure better protection of privacy; and,

32.5. Equality: consider that all measures intended to restrict anonymity must not be discriminatory against specific individuals or groups to prevent any disproportionate impact on marginalized groups and secure the right to equality and non-discrimination.