Warsaw, 13 October 2020
Opinion-Nr.: GEN-UKR/380/2020 [AIC]

OPINION ON THE DRAFT LAW AMENDING THE LAW "ON THE SECURITY SERVICE OF UKRAINE"

UKRAINE

This Opinion has benefited from contributions made by Mr. Sami Faltas, Independent Expert on Security Sector Reform; Mr. Ian David Leigh, Professor of Law, Durham University, United Kingdom; Ms. Nazli Yildirim Schierkolk, Independent Expert on Security Sector Reform; and the OSCE Conflict Prevention Centre and the Strategic Police Matters Unit, Transnational Threats Department, of the OSCE Secretariat.

Based on an unofficial English translation of the Draft Concept provided by the Security Service of Ukraine.

OSCE Office for Democratic Institutions and Human Rights

Ul. Miodowa 10, PL-00-251 Warsaw
Office: +48 22 520 06 00, Fax: +48 22 520 0605
www.legislationline.org

EXECUTIVE SUMMARY AND KEY RECOMMENDATIONS

ODIHR welcomes Ukraine's willingness to reform its Security Service (SSU) and to seek international expertise on the Draft Law to ensure its compliance with international human rights standards. However, several provisions of the Draft Law may potentially lead to dangerous interference with human rights and fundamental freedoms and lack substantive and procedural safeguards required according to international standards and recommendations.

Overall, in the absence of a clear, precise and exhaustive legal definition of national security threats, SSU's mandate is potentially overbroad and subject to arbitrary interpretation. While it is welcome to describe in details the nature of SSU's powers, the said powers seem to extend far beyond those normally granted to security services in other European countries. ODIHR therefore reiterates the recommendation made in its *ODIHR Opinion on the Draft Concept on the Reform of the Security Service of Ukraine* to remove any law enforcement functions and limit SSU's mandate to intelligence and counter-intelligence activities. Moreover, a number of the more intrusive powers granted to the SSU lack the *ex ante* and *ex post facto* safeguards that would be expected under international human rights law and according to good practices.

Further, the Draft SSU Law does not really elaborate the provisions on oversight and more details regarding accountability and the mandate and powers of oversight mechanisms should be provided to ensure that they are able to carry out their functions in the most proficient and effective manner. In addition, gender and diversity should be mainstreamed throughout the Draft Law to ensure that they are promoted internally as part of the working culture of the SSU, as well as externally when delivering security services.

More specifically, and in addition to what is stated above, ODIHR makes the following recommendations to further enhance the Draft Law:

A. to revise the scope of the mandate and powers of the SSU:

1. by removing from SSU's mandate the fight against organized crime, corruption, economic crimes, administrative offences and border and migration management-related activities, or, if retained at all, specifying that SSU is involved only when these behaviours pose a clear and present danger to national security, and more generally ensure that SSU's mandate is systematically linked to the protection of national security, while ensuring that the constituting elements and threats to national security are strictly, clearly and exhaustively defined; [pars 14-17, 36-41 and 43]
2. by revising SSU's mandate to ensure that
   - it is limited to intelligence/counter-intelligence activities, thereby removing any law enforcement functions (such as the use of coercive measures, criminal investigations, arrest and detention, search, seizure and powers of interrogation) from the scope of the powers of the SSU and transfer them to the police and other competent authorities, as appropriate;
   - or if deemed an absolute necessity and retained, the scope and application of such law enforcement and investigative powers are strictly limited and exclusively used for combatting certain clearly defined national security criminal

offences, when there is a reasonable suspicion that an individual has committed or is about to commit such offences or related preparatory/inchoate offences;
- other law enforcement bodies shall not exercise law enforcement powers in relation to the same offences; and
- the exercise of these powers by the SSU is subject to the same legal safeguards and oversight that apply to other law enforcement agencies, providing that they are compliant with international human rights standards; [pars 11, 96-105]

3. by, if pre-trial investigations powers are retained, explicitly spelling out that the respective SSU activities shall be carried out in full compliance with the requirements of the Criminal Procedure Code, whenever relevant; [par 52]
4. by removing from Article 216 of the Criminal Procedure Code the power of the Head of the SSU to request the transfer of a case from the prosecutorial authorities; [par 55]
5. by expressly stating that the SSU should not be permitted to deprive persons of their liberty simply for the purpose of intelligence collection nor to operate its own detention facilities or to make use of any unacknowledged detention facilities operated by third parties; [par 102]

B. to ensure that the Draft SSU Law or other relevant legislation clearly and strictly specifies the personal, material and temporal scope of SSU's targeted surveillance powers as well as substantive and procedural safeguards for conducting covert surveillance, including judicial authorization, oversight of information collection measures (supervision of investigations, ordering the termination of surveillance and ordering the destruction of data collected) and ex-post adjudication of cases [pars 59-64]

C. to clearly and strictly circumscribe the SSU's powers to conduct mass surveillance, by specifying the permissible objectives, duration and renewal of such measures, as well as providing for robust independent oversight of the entire selection process, including the selection of bearers for interception, the selectors and search criteria for filtering intercepted communications, and the selection of material for examination by an analyst; [par 68]

D. to provide for detailed procedures on how telecommunication interception should be requested, reviewed, authorised, implemented and overseen, [par 70] while clearly stipulating in the Draft Law or other legislation the procedures for examining, using, and storing the data intercepted by the SSU, the precautions to be taken when communicating the data to other parties, the duration (not excessively long) of such measures and the circumstance in which recordings may or must be erased or destroyed; [par 74]

E. to revise Articles 13.3, 14.1 and 14.2 of the Draft SSU Law by more strictly circumscribing and elaborating the procedures and safeguards applicable to information sharing between the SSU and other domestic agencies; [par 93]

F. to regulate more strictly international information and intelligence sharing agreements or practices by requiring an assessment of the counterpart's record on human rights and data protection and related legal and institutional framework, while prohibiting the transfer of intelligence likely to be used for purposes that violate human rights,

and ensuring that oversight bodies have the explicit mandate to scrutinize international intelligence co-operation, including the compliance with the Ukrainian legislation and international human rights standards of agreements and security service co-operation with foreign bodies, the exchange of information, joint operations and the provision of equipment and training; [par 95]

G. to specify the grounds for dismissal of the Head of the SSU stated in Article 10.10 (5) of the Draft Law, as they relate to the "*systematic failure to perform their official duties*" or showing "*inaptitude*"; [par 47]

H. to ensure that oversight not only focuses on the "*activities of the SSU*" but covers all aspects of the SSU's functioning and work (including but not limited to the compliance with the law and international human rights standards, the effectiveness and efficiency of their activities, gender and diversity, their finances and their administrative practices), while defining more clearly the scope, mandate and powers of the different control and oversight mechanisms and guaranteeing that they all have a right to access to all (classified) information relevant to their functions and necessary to discharge their responsibilities on the basis of procedure clearly defined by law; [pars 113, 117-134]

I. to further elaborate, in Article 47.3, the oversight mandate of the Parliamentary Committee, especially in relation to specific aspects of the work of security services, such as overseeing information collection measures, co-operation and information exchange with foreign services, the use of personal data, as well as the handling of individual complaints against security services; [par 120]

J. to detail the scope and extent of judicial oversight, both in terms of *a priori* and *ex post facto* control, in particular with regard to the authorization of surveillance, the ongoing oversight/follow-up control of information collection measures and *ex-post* adjudication of cases; [par 129]

K. to supplement Articles 49 and 50 to detail the mechanisms and procedures of internal control to ensure that the services operate in compliance with laws and human rights standards, with particular emphasis on internal review and authorization of surveillance measures and of other methods that infringes upon human rights, as well as more generally, to ensure compliance with human rights standards, while also providing for internal complaint channels and the protection of whistle-blowers as an important internal control mechanism; [par 132]

L. to provide that SSU personnel incur liability for violation of criminal, administrative and civil law, and international human rights law and include clear rules and procedures to prevent and detect unacceptable practices; [par 164] and

M. to enhance the provisions concerning gender, diversity and non-discrimination to ensure that gender and diversity are promoted internally as part of the working culture of the institution, as well as externally when delivering security services, and when budgeting and carrying out oversight. [see detailed recommendations in pars 12, 46, 99, 113, 126, 134, 147-156, 179 and 182]

These and additional Recommendations, as highlighted in bold, are included throughout the text of this Opinion.

As part of its mandate to assist OSCE participating States in implementing OSCE commitments, the OSCE/ODIHR reviews, upon request, draft and existing legislation to assess their compliance with international human rights standards and OSCE commitments and provides concrete recommendations for improvement.

TABLE OF CONTENT

I. INTRODUCTION

1. On 12 February 2020, the OSCE Project Co-ordinator in Ukraine forwarded to the OSCE Office for Democratic Institutions and Human Rights (ODIHR) a request from the Chair of the Security Service of Ukraine (SSU) to review the *Draft Concept on the Reform of the Security Service of Ukraine* (hereinafter "the Draft Concept").
2. On 27 March 2020, ODIHR received a second request from the Chair of the SSU to review the *Draft Law of Ukraine on Incorporating Amendments into the Law "On the Security Service of Ukraine"* (hereinafter "the Draft Amendments"). The Draft Amendments include an amended version of the *Law "On the Security Service of Ukraine"* (hereinafter "the Draft SSU Law") as well as amendments to various other codes and laws.[1]
3. ODIHR agreed to prepare two legal reviews on the Draft Concept and on the Draft Amendments respectively, to assess their compliance with OSCE human dimension commitments and international human rights standards, which should be read together.[2]
4. This Opinion was prepared in response to the above request. ODIHR conducted this assessment within its mandate to assist OSCE participating States in the implementation of key OSCE commitments in the human dimension.

II. SCOPE OF REVIEW

5. The scope of this Opinion covers only the Draft Amendments submitted for review. Thus limited, the Opinion does not constitute a full and comprehensive review of the entire legal and institutional framework regulating the SSU, though it should be read together with the *ODIHR Opinion on the Draft Concept on the Reform of the Security Service of Ukraine (19 august 2020).*
6. The Opinion raises key issues and provides indications of areas of concern. In the interest of conciseness, the Opinion focuses more on those provisions that require improvements than on the positive aspects of the Draft Amendments. The ensuing recommendations are based on international and regional standards, norms and practices as well as relevant OSCE human dimension commitments. The Opinion also highlights, as appropriate, good practices from other OSCE participating States in this field.
7. Moreover, in accordance with the *Convention on the Elimination of All Forms of Discrimination against Women*[3] (hereinafter "CEDAW") and the *2004 OSCE Action*

[1] These include amendments to the Code on Administrative Offences, the Criminal Code, the Civil Procedure Code, the Air Code, the Criminal Procedure Code, the Laws "On Detective Operations", "On Pensions of Military Retirees and Some Other Persons", "On Organisational and Legal Foundations of Combating Organised Crime", "On Mobilisation Preparation and Mobilisation", Ukraine "On Status of War Veterans, Guarantees of Their Social Protection", "On State Protection of Employees of Courts and Law Enforcement Agencies", "On Status and Social Protection of Veterans of Military Service, Veterans of Internal Affairs Bodies, Veterans of the National Police and Some Other Persons", "On Counterintellingence Activities", "On State Control over International Transfer of Military and Dual Use Goods", "On Burials and Funeral Business", "On Telecommunications", "On State Targeted Programmes", "On International Treaties of Ukraine", "On Military Duty and Military Service", "On Personal Data Protection", "On Access to Public Information", "On Prevention of Corruption", "On Transparent Use of Public Funds", "On National Security of Ukraine" and "On Incorporating Amendments into Some Laws of Ukraine re Resetting of Power".

[2] The *2020 ODIHR Opinion on the Draft Concept on the Reform of the SSU* (19 August 2020) is available at: <https://www.legislationline.org/odihr-documents/page/legal-reviews/country/52/Ukraine/show>.

[3] *UN Convention on the Elimination of All Forms of Discrimination against Women* (hereinafter "CEDAW"), adopted by General Assembly resolution 34/180 on 18 December 1979. Ukraine deposited its instrument of ratification of this Convention on 12 March 1981.

Plan for the Promotion of Gender Equality[4] and commitments to mainstream a gender perspective into OSCE activities, programmes and projects, the analysis seeks to take into account the potentially different impact of the Draft Amendments on women and men, both as recipients of intelligence services as well in their function to deliver intelligence services and manage decisions related to them.

8. The Opinion is based on an unofficial English translation of the Draft Amendments provided by the SSU, which is attached to this document as an Annex. Errors from translation may result. The Opinion is also available in Ukrainian. However, the English version remains the only official version of the Opinion.

9. In view of the above, ODIHR would like to stress that this review does not prevent ODIHR from formulating additional written or oral recommendations or comments on respective policy or related legislation regulating the SSU in the future.

III. ANALYSIS AND RECOMMENDATIONS

1. Relevant International Standards and OSCE Human Dimension Commitments

10. For a detailed overview of international standards and OSCE commitments relevant to security sector reform,[5] and more specifically the security service, ODIHR hereby refers to Section III.1 on the International Standards and OSCE commitments of its *ODIHR Opinion on the Draft Concept on the Reform of the Security Service of Ukraine*.

---

[4] See *OSCE Action Plan for the Promotion of Gender Equality*, adopted by Decision No. 14/04, MC.DEC/14/04 (2004), par 32.

[5] These include the International Covenant on Civil and Political Rights (ICCPR), ratified by Ukraine on 12 November 1973; the European Convention on Human Rights and Fundamental Freedoms (ECHR), ratified by Ukraine on 11 September 1997. In addition, Ukraine has also ratified, among others, the UN Convention on the Elimination of All Forms of Discrimination against Women (CEDAW), the UN Convention on the Elimination of All Forms of Racial Discrimination (CERD), the UN Convention on the Rights of Persons with Disabilities (CRPD), the UN Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (UNCAT) and the Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (CETS No.. 108), 28 January 1981 (ratified by Ukraine on 30 September 2010 and which entered into force on 1 January 2011); and Council of Europe, *Convention on Access to Official Documents* (CETS No. 205), 18 June 2009, signed by Ukraine on 12 April 2018, but not yet ratified. At the OSCE level, see *1975 Helsinki Final Act 1975* (Questions Relating to Security in Europe: 1.(a) Declaration on Principles Guiding Relations between Participating States, Principle VII); *1990 Copenhagen Document*, Preamble and pars 1 and 41; *1992 Helsinki Document* (Summit Declaration), par 21; *1994 Budapest Document* (Summit Declaration), par 14; *2003 Maastricht Document* (*OSCE Strategy to Address Threats to Security and Stability in the Twenty-First Century; Threats to security and stability in the twenty-first century*), pars 4 and 9; *2010 Astana Commemorative Declaration: Towards a Security Community*, pars 2 and 6. Other non-binding relevant documents include: OSCE Secretary General, *Report on the OSCE Approach to Security Sector Governance and Reform* (SSG/R) (2019); 1994 *OSCE Code of Conduct on Politico-Military Aspects of Security;* DCAF – OSCE/ODIHR and UN Women, *Gender and Security Toolkit* (2019), especially *Tool no. 14 on Intelligence and Gender*. Other specialized documents of a non-binding nature, which have been endorsed in various international or regional fora and may prove useful as they contain a higher level of details, such as UN Special Rapporteur on the protection and promotion of human rights while countering terrorism (UN SRCT), *Compilation of Good Practices on Legal and Institutional Frameworks and Measures that Ensure Respect for Human Rights by Intelligence Agencies while Countering Terrorism, including on their Oversight (2010)* (hereinafter "UN SRCT Compilation"), developed by the, as mandated by the UN Human Rights Council; CoE Commissioner for Human Rights, *Issue Paper on Democratic and Effective Oversight of National Security Services*, (2015); CoE Parliamentary Assembly (PACE), *Recommendation 1402 (1999) on the Control of Internal Security Services in Council of Europe Member States* (1999); *Recommendation 1713 (2005) on Democratic Oversight of the Security Sector in the Member States* (2005); *Resolution 1838 (2011) on Abuse of State Secrecy and National Security: Obstacles to Parliamentary and Judicial Scrutiny of Human Rights Violations* and *Resolution 2060 on Improving the Protection of Whistleblowers* (2015); CoE, European Commission for Democracy through Law (Venice Commission), *Report on the Democratic Oversight of the Security Services*, CDL-AD(2015)010; *Report on the Democratic Oversight of Signals Intelligence Agencies*, CDL-AD(2015)011; *2015 Update of the 2007 Report on the Democratic Oversight of the Security Services and Report on the Democratic Oversight of Signals Intelligence Agencies*, CDL-AD(2015)006; and 2007 *Report on the Democratic Oversight of the Security Services*, CDL-AD(2007)016; NATO Parliamentary Assembly-DCAF, Yildirim Schierkolk, Nazli, *Parliamentary Access to Classified Information* (2018); European Parliament, Committee on Civil Liberties, Justice and Home Affairs, *Study on the Parliamentary Oversight of Security and Intelligence Agencies in the European Union* (2011); European Union Agency for Fundamental Rights (FRA), *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU - Mapping Member States' legal frameworks* (2015); the *Global Principles on National Security and the Right to Information* (2013 Tshwane Principles), developed and adopted on 12 June 2013 by a large assembly of experts from international organizations, civil society, academia and national security practitioners.

2. GENERAL COMMENTS

2.1. Overall Recommendations

11. At the outset, ODIHR would like to underline that several of the recommendations made with regard to the *Draft Concept on the Reform of the SSU* are similarly applicable in the case of the Draft Amendments and will not be reiterated *in extenso* in this Opinion, including:

- with regards to the SSU's law enforcement mandate and powers,[6] ODIHR reiterates its recommendation to remove any law enforcement functions, such as criminal investigations, use of coercive measures, arrest and detention, from the scope of the powers of the SSU in the Draft Amendments and to limit SSU's mandate to intelligence and counter-intelligence activities; or if deemed an absolute necessity and retained at all, strictly limit the scope and application of such law enforcement powers exclusively for combatting certain clearly defined national security criminal offences, when there is a reasonable suspicion that an individual has committed or is about to commit such offences or related preparatory/inchoate offences; specify that other law enforcement bodies shall not exercise law enforcement powers in relation to the same offences; and ensure that the exercise of these powers by the SSU is subject to the same legal safeguards and oversight that apply to other law enforcement agencies; (see Sub-Section 4.1 of the *ODIHR Opinion on the Draft Concept*)
- the importance of having the Draft Amendments refer to both state and human security, whenever appropriate, to emphasize that security services should fulfil their mandates in a manner that serves the interests of the State *and* society as a whole;[7] (see Sub-Section 2.1 of the *Opinion on the Draft Concept*)
- while a few provisions of the Draft Amendments make some references to "*respect for human rights and fundamental freedoms*", and "*ensuring humane treatment of people*",[8] which is welcome,[9] it should be expressly stated that the SSU shall not only respect human rights but also protect them, and comply with international law *and human rights* obligations binding on Ukraine and that SSU personnel will incur liability in case of violation; (see Sub-Section 2.2 of the *Opinion on the Draft Concept* and Sub-Section 6.4 *infra*)
- in terms of operational principles listed in Article 5 of the Draft SSU Law, it may be advisable to reiterate the principle of good governance (while specifying what this entails in terms of accountability, transparency, rule of law, participation, responsiveness, effectiveness and efficiency),[10] to complement the wording "*responsibility to the people of Ukraine*" with the broader principle of "*democratic and civilian oversight*" and what this entails, adding the principles of "*individual responsibility*" and "*professionalism*",[11]

---

[6] The SSU is defined as "*a state special-purpose law enforcement authority that ensures state security of Ukraine*" (see e.g., Article 2.1 of the Draft SSU Law and amended Article 19.1 of the Law on National Security of Ukraine) and granted extensive law enforcement and policing powers (see e.g., Articles 2, 3 and 12 of the Draft SSU Law).

[7] *Op. cit.* footnote 5, par 18 (2010 UN SRCT Compilation).

[8] See e.g., Articles 2.2 and 35.3 of the Draft SSU Law and draft amended Article 19.2 (5) of the Law on National Security of Ukraine

[9] *Op. cit.* footnote 5, par 12 (2010 UN SRCT Compilation).

[10] See e.g., *op. cit.* footnote 5, pages 13-14 (2019 DCAF-OSCE/ODIHR-UN Women Tool no. 1 on SSG/SSR and Gender), which refer to "*Accountability: the security sector must be held accountable for meeting the diverse needs of all sectors of the population; Transparency: information is freely available and accessible to those who will be affected by decisions and their implementation; Rule of law: all persons and institutions, including the state, are subject to laws that are known publicly, enforced impartially and consistent with international and national human rights norms and standards; Participation: all persons of all backgrounds have the opportunity to participate in decision-making and service provision on a free, equitable and inclusive basis, either directly or through legitimate representative institutions; Responsiveness: institutions are sensitive to the different security needs of all parts of the population, and perform their missions in the spirit of a culture of service and without discrimination; Effectiveness: institutions fulfil their respective roles, responsibilities and missions to a high professional standard according to the diverse needs of all parts of the population; and Efficiency: institutions make the best possible use of public resources in fulfilling their respective roles, responsibilities and missions".*

[11] *Op. cit.* footnote 5, Practice 19 (2010 UN SRCT Compilation).

and replacing the wording "*optimal balance between transparency and secrecy*" by a reference to openness, transparency and accessibility, subject to strictly necessary and proportionate exceptions for the sake of national security (see pars 31-36 and 41 of the *Opinion on the Draft Concept*).

12. Moreover, apart from a reference in Article 5.1 (4) of the Draft SSU Law to "*equality of all before the law*" as one of the operational principles of the SSU, there is no other provisions in the Draft SSU Law reflecting or addressing gender and diversity considerations and non-discrimination. In line with the recommendations provided in the *Opinion on the Draft Concept*, the Draft Amendments should be supplemented in that respect particularly by:

- providing a concrete mechanism for achieving greater gender balance and diversity within SSU's workforce, including decision-making positions, based on a proper assessment (or explicitly refer to the development of policy or secondary legislation for that purpose);[12]
- introducing measures to ensure the retention, professional development and promotion of all staff, including women and under-represented persons/groups;[13]
- specifically requiring the SSU to develop human resource policies that take into consideration the needs of pregnant women and persons with parental and/or caretaking responsibilities,[14] as well as the special requirements for employees with disabilities, in line with Article 27 of the UN Convention on the Rights of Persons with Disabilities;[15]
- explicitly prohibiting discrimination against individuals or groups on the grounds of their national or ethnic origin, color, language, religion or belief, political or other opinion, social origin, sex, sexual orientation or gender identity, or other status,[16] both in terms of internal policies and functioning of the SSU as well as its external operational activities where the SSU should not discriminate in law or practice against anyone on any ground;[17]

[12] The *OSCE Decision no. 7/09 on "Women's participation in political and public life"* calls upon OSCE participating States to "*[c]onsider providing for specific measures to achieve the goal of gender balance in all legislative, judicial and executive bodies, including security services*" (par 1). Special temporary recruitment measures might be considered in order to quickly redress an imbalance (see e.g., Committee on the Elimination of All Forms of Discrimination against Women, *General recommendation No. 25 on Article 4 par 1 of the Convention on the Elimination of All Forms of Discrimination against Women on Temporary Special Measures*, pars 21-22; see also *op. cit.* footnote 5, pages 5 and 37 (2019 DCAF-OSCE/ODIHR-UN Women Tool no. 14 on Intelligence and Gender)). It is understood from the SSU's website that about one third of the employees of the SSU are women, including about three hundred holding senior positions (see <https://ssu.gov.ua/ua/pages/354>). A number of OSCE participating States have mainstreamed gender throughout their public services, including their intelligence services, and report having achieved gender balance in staffing (see e.g., *op. cit.* footnote 5, page 2 (2019 DCAF-OSCE/ODIHR-UN Women Tool no. 14 on Intelligence and Gender)).

[13] *OSCE Decision no. 7/09 on "Women's participation in political and public life"*, par 4, which states that OSCE participating States should "*take measures to create equal opportunities within the security services, including the armed forces, where relevant, to allow for balanced recruitment, retention and promotion of men and women*".

[14] *OSCE Decision no. 7/09 on "Women's participation in political and public life"*, par 9, which states that OSCE participating States should "*[e]ncourage shared work and parental responsibilities between women and men in order to facilitate women's equal opportunities to participate effectively in political and public life*". See also e.g., *op. cit.* footnote 5, page 34 (2019 DCAF-OSCE/ODIHR-UN Women Tool no. 14 on Intelligence and Gender)..

[15] UN Convention on the Rights of Persons with Disabilities, adopted on 13 December 2006 during the sixty-first session of the UN General Assembly by resolution A/RES/61/106; the Convention was ratified by Ukraine on 4 February 2010.

[16] *Op. cit.* footnote 5, Practice 11 (2010 UN SRCT Compilation).

[17] ibid. Practice 11 (2010 UN SRCT Compilation).

- explicitly prohibiting the unlawful collection and automatic processing of personal (sensitive) data[18] as well as discriminatory (e.g., religious or ethnic) profiling,[19] ensuring that SSU's activities (e.g., information gathering or surveillance) is undertaken on the basis of individuals' behaviour, and not on prohibited characteristics;[20]
- expressly providing that the SSU management or human resources department shall develop secondary legislation or specific policy to build an institutional culture and work practices that are inclusive, non-discriminatory and open to diversity in policy as well as in practice;[21]
- explicitly prohibiting sexual, gender-based and other types of abuse or harassment, sexism, bullying, exploitation, violence or discrimination based on gender, sexual orientation, gender identity, gender expression or any other ground, within the institution and when delivering security services, while ensuring that proper and functioning non-discriminatory, gender-responsive and accessible reporting, complaints and disciplinary mechanisms are in place to prohibit, prevent, detect and respond effectively to such cases, while protecting complainants from retaliation;[22] such mechanisms must be designed in ways that protect complainants from retaliation by those accused of wrongdoing or by senior staff;[23]
- ensuring that training of SSU personnel includes gender, diversity and human rights training,[24] e.g., in Article 36 of the Draft SSU Law;
- specifically mentioning as a key responsibility of the SSU Management (for instance under Article 10.4 of the Draft SSU Law) the promotion of gender and diversity within the SSU at all levels and when delivering services;
- ensuring that oversight bodies have appropriate mandates, powers, capacity and resources to enable them to undertake a systemic examination of gender and diversity issues both regarding internal intelligence services' functioning and staffing and when they carry out their activities;[25] and

---

[18] These include e,g, "*personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation*" as per Article 10 of the Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119 (Police Directive), which also states that "*"[p]rofiling that results in discrimination against natural persons on the basis of special categories of personal data referred to in Article 10 shall be prohibited, in accordance with Union law"* (Article 3 (4)). Article 6 of the *CoE Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (ETS no. 108) also provides that "*personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards*". See also ODIHR, *Guidelines on Addressing the Threats and Challenges of "Foreign Terrorist Fighters"* (2018), pages 62-63; and ODIHR, *Guidebook on Preventing Terrorism and Countering Violent Extremism and Radicalization that Lead to Terrorism: A Community-Policing Approach* (2014), pages 56-60; and EU Fundamental Rights Agency, *Guidebook on Preventing Unlawful Profiling* (2018). See also UN Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, *Report on Racial and Ethnic Profiling*, A/HRC/29/46, 20 April 2015, par 66. See e.g., CERD, *General Recommendation No. 34 on Racial Discrimination against People of African Descent*, par 39. In the context of policing, see also ODIHR, *Opinion on the Draft Law of Ukraine on Police and Police Activities* (2014), par 30; and Council of Europe's European Commission against Racism and Intolerance (ECRI), *General Policy Recommendation No. 11 on Combating Racism and Racial Discrimination in Policing*, 29 June 2007.

[19] International Mandate-Holders on Freedom of Expression, *2016 Joint Declaration on Freedom of Expression and Countering Violent Extremism*, par 2 (g), which states that "*States should never base surveillance on ethnic or religious profiling or target whole communities, as opposed to specific individuals, and they should put in place appropriate legal, procedural and oversight systems to prevent abuse of surveillance powers*".

[20] *Op. cit.* footnote 5, par 18 (2010 UN SRCT Compilation). See also CERD, *General Recommendation No. 30 on Discrimination Against Non-citizens* (2004), par 10.

[21] *Op. cit.* footnote 2, pars 86-95 (2020 ODIHR Opinion on the Draft Concept on the Reform of the SSU).

[22] *Op. cit.* footnote 5, Practice 18 (2010 UN SRCT Compilation); page 37 (2019 DCAF-OSCE/ODIHR-UN Women Tool no. 1 on SSG/SSR and Gender); and page 39 (2019 DCAF-OSCE/ODIHR-UN Women Tool no. 14 on Intelligence and Gender). For guidance on gender and internal complaints mechanisms, see e.g., DCAF, Megan Bastick, *Gender and Complaints Mechanisms: A Handbook for Armed Forces and Ombuds Institutions to Prevent and Respond to Gender-Related Discrimination, Harassment, Bullying and Abuse* (2015). See also OSCE/ODIHR-DCAF-OSCE Gender Section, *Guidance notes on Integrating a Gender Perspective into Internal Oversight within Armed Forces, on Integrating Gender into Internal Police Oversight, and on Integrating Gender into Oversight of the Security Sector by Ombuds Institutions & National Human Rights Institutions* (2014).

[23] ibid. page 33 (2019 DCAF-OSCE/ODIHR-UN Women Tool no. 14 on Intelligence and Gender).

[24] DCAF-UNDP, *Public Oversight of the Security Sector - A Handbook for Civil Society Organizations* (2008), page 225.

[25] ibid. page 33 (2019 DCAF-OSCE/ODIHR-UN Women Tool no. 14 on Intelligence and Gender).

- increasing the participation of women and other under-represented groups in decision-making processes related to the work of the security services (both strategic and operational) as well as in security sector legislative reform processes (see also Sub-Section 9 *infra* on the reform process).

2.2. Definition of Terms

13. Article 1 of the Draft SSU Law and amended Article 1 of the Law on National Security provide a series of vague, complex and overlapping definitions in relation to the objectives and functions of the SSU, e.g., "*state security threats*", "*state security*", "*national security*", "*national values*", "*national interests*" and "*fundamental national values*". Unless this is due to translation inaccuracies, these terms seem to be used without consistency, and at times the definitions appear circular and/or are open-ended.[26] In particular, the Draft Law seems to use "national security" or "state security" interchangeably without defining clearly and precisely the scope and meaning of the protected interests. Some of these provisions, for instance the definition of "*national values*", are so all-embracing that virtually every aspect of national, economic, cultural and social life could potentially come within the sights of the SSU. Overall, the said definitions do not bring a clear list of what national security threats are, which has important consequences since the way such threats are defined in national legislation shapes the scope of the SSU's mandate and powers. Other terms[27] are so vague and broadly framed that they could potentially enable the SSU to act against organizations and persons, including journalists, that have not broken the law and whose behaviours do not necessarily constitute a clear and present danger to the security of Ukraine, but which activities are considered to be critical of state authorities and therefore potentially destabilizing.

14. Given the risk of SSU's powers to interfere with human rights, the underlying framework must satisfy the principle of legal certainty. This means that the law must be adequately accessible, clear and foreseeable, i.e. formulated with sufficient precision to enable the individual to regulate his or her conduct accordingly.[28] This is also important to prevent arbitrariness in their application.[29] **It is thus essential that the Draft Amendments clearly define national security threats, while avoiding vague and overbroad formulations, such as "*national values*", "*national interests*" and "*fundamental national values*".**

15. It must be acknowledged that national security threats thereto are not easy to define and they remain in an area where countries enjoy a certain margin of appreciation, based on

[26] For instance, Article 12.1 of the Draft SSU Law gives power to undertake various activities while performing the SSU "*functions*", which are defined in Article 3 with reference to the concept of "*state security*". "*State security"* in turn is defined in the amended Article 1.4 of the Law on National Security with reference to "*the foundations of national security*", "*national values*" and so-called "*relevant national interests"* and "*requisite national goals*". "*National security*" is then further defined in amended Article 1.9 of the same Law in a circular fashion, referring back to "*national interests*", "*national goals"* and "*national values*", which are then defined in Articles 1.10 to 1.12 respectively. The definition of "*national interests"* then refers to "*vital needs*" of the Ukrainian people (not defined), while "*national goals"* (Article 1.11) cross-refers again in a circular way to '*national interests"* and "*national values*'. Amended Article 1.12 of the Law on National Security provides a definition of "*national values*" including, among other matters, citizens' welfare, law and order, social justice and the material, intellectual and spiritual heritage of the Ukrainian people "*as well as other values that ensure the self-preservation, sustainable and progressive development of the Ukrainian people, society and the State*", which beyond being open-ended also appears vague and extremely broad. The proposed new Articles 3-1 to 3-5 of the Law on National Security of Ukraine further elaborate such definitions, while specifying that the proposed lists are not exhaustive.

[27] For instance: "*subversive acts (exerting influence on societal relations that poses or can pose a threat to state security and/or increases state security risks) carried out by foreign special services, as well as organisations, institutions, forces, groups, structures, entities or individuals*".

[28] ECtHR, *Weber and Saravia v. Germany* (Application no. 54934/00, judgment of 29 June 2006), par 84; *The Sunday Times v. the United Kingdom* (no. 1) (Application no. 6538/74, judgment of 26 April 1979), par 49; and *Shvydka v. Ukraine* (Application no. 17888/12, judgment of 30 October 2014), par 39. See also e.g., European Commission for Democracy through Law (Venice Commission), *Rule of Law Checklist*, CDL-AD(2016)007, 18 March 2016, Part II.B.3.

[29] ECtHR, *Malone v. the United Kingdom* (Application no. 8691/79, judgment of 2 August 1984), par 67, where the ECtHR emphasized that there must be "*a measure of legal protection in domestic law against arbitrary interferences by public authorities with the rights safeguarded by the Convention*".

their unique geopolitical and security circumstances and the differing security needs and expectations of all individuals, including women, men, girls, boys and persons from marginalized groups.[30] Some countries clearly define national security and threats attached, either in legislation or strategic policy documents.[31]

16. While there is no binding international legal standard establishing the scope of mandate of security services, their mandates should be *"strictly limited to protecting legitimate national security interests as outlined in publicly available legislation or national security policies and identify the threats to national security that intelligence services are tasked to address"*.[32] According to the *Compilation of Good Practices on Legal and Institutional Frameworks and Measures that Ensure Respect for Human Rights by Intelligence Agencies while Countering Terrorism* (2010) developed by the UN Special Rapporteur on the protection and promotion of human rights while countering terrorism (UN SRCT Compilation), the main purpose of security services is generally to *"[c]ollect, analyze and disseminate information that assists policymakers and other public entities in taking measures to protect national security*".[33] The UN SRCT Compilation further underlines that *"[i]f terrorism is included among these threats, it [should be] defined in narrow and precise terms*".[34] The Parliamentary Assembly of the Council of Europe defines "*protecting national security*" as "*combating clear and present dangers to the democratic order of the state and its society*", excluding economic objectives or organized crime except if they present a clear and present danger to national security.[35] The jurisprudence of the ECtHR so far does not recognize organized crimes *per se* as a threat to national security.[36]

17. In light of the foregoing, in the absence of a clear, precise and exhaustive legal definition of national security threats, SSU's mandate is overbroad and subject to potential arbitrary interpretation. **It is thus recommended to better streamline the definitions, while refraining from using vague and overbroad terminology and open-ended formulation and circular definitions, and excluding organized crimes and economic**

---

[30] The ECtHR in several rulings stated that « [b]y the nature of things, threats to national security may vary in character and may be unanticipated or difficult to define in advance » ; see e.g., ECtHR, *Al-Nashif v. Bulgaria* (Application no. 50963/99, judgment of 20 June 2002), though it also ruled that "that does not mean that its limits may be stretched beyond its natural meaning" (ECtHR, *C.G. and others v. Bulgaria* (Application no. 1365/07, judgment of 24 April 2008), par 43). The ECtHR has recognized the following as threats to national security: espionage (*Roman Zakharov v. Russia* (2015); *Klass v. Germany (1978)*); terrorism (*Klass v. Germany (1978)*, *Weber and Saravia v. Germany (2006)*); incitement to/approval of terrorism (*Zana v. Turkey* (1997)); subversion of parliamentary democracy (*Leander v. Sweden* (1987)); so-called "separatist extremist" organisations that threaten the unity or security of a state by violent or undemocratic means (*United Communist Party of Turkey v. Turkey (1998)*); inciting disaffection of military personnel (*Arrowsmith v. United Kingdom (1977)*). See also European Union Agency for Fundamental Rights (EU FRA), *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU* - Volume II: field perspectives and legal update (Luxembourg, 2017), page 53.

[31] See for instance, in the **United Kingdom** (UK), *UK National Security Strategy*, p.27, which includes a clear and comprehensive list of risks to UK National Security, divided in three priority tiers; **Canada**, the Canadian Security Intelligence Service (CSIS) is mandated to "*collect, by investigation or otherwise, to the extent that it is strictly necessary, and analyze and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada and, in relation thereto, shall report to and advise the Government of Canada*" (see *Canadian Security Intelligence Service Act* (CSIS) (R.S.C., 1985, c. C-23), Sections 12(1) and 2 of the CSIS Act lists in detail what is meant by "*threat to the security of Canada*" i.e., "*(a) espionage or sabotage that is against Canada or is detrimental to the interests of Canada or activities directed toward or in support of such espionage or sabotage; b) foreign influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person; (c) activities within or relating to Canada directed to- ward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political, religious or ideological objective within Canada or a foreign state, and; d) activities directed toward undermining by covert unlawful acts, or directed toward or intended ultimately to lead to the destruction or overthrow by violence of, the constitutionally established system of government in Canada";* **Luxembourg** defines national security threats as: "*activity which threatens or could threaten the national security or the above-mentioned interests, every activity, individual or collective, deployed domestically or from abroad, a) which can be related to espionage, interference, terrorism, violent propensity extremism, proliferation of arms of mass destruction or of products linked to defence and technology related to defence, organised crime or cyber-threat to the extent that the latter two are linked to previously mentioned activities, and b) which is likely to endanger the independence and sovereignty of the State, the security and functioning of institutions, fundamental rights and civil liberties, the security of individuals and goods, the scientific and technical potential or the economic interests of the Grand Duchy of Luxembourg*" (see *Law of 5 July 2016*, Art. 3(2)).

[32] *Op. cit.* footnote 5, Practice 2 (2010 UN SRCT Compilation).

[33] ibid. Practice 1 (2010 UN SRCT Compilation).

[34] ibid. Practice 2 (2010 UN SRCT Compilation).

[35] See *op. cit.* footnote 5, par A.2 (1999 PACE Recommendation 1402)

[36] See e.g., ECtHR, *C.G. and others v. Bulgaria* (Application no. 1365/07, judgment of 24 April 2008), pars 40-43, where the Court rules that "*involvement in drug trafficking"* in the context of the case concerned, cannot be considered as a threat to national security.

objective from the scope of security threats (except if they present a clear and present danger to national security) (see also Sub-Section 3 on SSU's general mandate).

2.3. Access to Information and State Secrets

18. Article 1 of the Draft SSU Law defines "secrecy" as the "*concealment of data on capabilities, actions, methods, forms, plans and intentions of the Security Service of Ukraine through the use of special means and tools for encrypting and denying access thereto in the manner prescribed by law*". This definition seems to be over-broad and potentially excludes a number of information that should in principle be in the public domain. Certain information may legitimately be classified on grounds of national security or protection of other overriding interests listed in Article 19 par 3 of the ICCPR and Article 10 par 2 of the ECHR.[37] At the same time, as noted in the *ODIHR Guidelines on the Protection of Human Rights Defenders*, national security is frequently used to justify the over-classification of information, thus limiting access to information of public interest and creating another obstacle for whistle-blowers and investigative journalists trying to bring to light alleged corruption and human rights violations by state actors.[38] Hence, **secrecy laws should define national security threats precisely** (see Sub-Section 2.2 *supra*) **and include narrowly and clearly defined prohibited disclosures, which are necessary and proportionate to protect national security**.[39]

19. As mentioned in par 11 *supra*, access to information and openness should be the starting point, and secrecy the exception. While it is beyond the scope of this Opinion to review and assess the *Law of Ukraine on the Protection of State Secrets*, it is important to state therein the key principles that should be respected by such legislation. The 2013 *Global Principles on National Security and the Right to Information* (The Tshwane Principles), as endorsed in Resolution 2060 of the Parliamentary Assembly of the Council of Europe (PACE),[40] can serve as useful guidance in that respect.[41]

20. Disclosure should not be limited in the absence of the Government's showing of "*a real and identifiable risk of significant harm to a legitimate national security interest*"[42] that outweighs the public's interest in the information to be disclosed[43] and any restrictions should be interpreted narrowly.[44] Secrecy legislation should indicate clearly the criteria, which should be used in determining whether or not information can be declared secret, so as to prevent abuse of the label "secret" for purposes of preventing disclosure of information which is in the public interest.[45] International good practices encourage the use of a list of categories of information, which should enjoy at least a high presumption in favour of disclosure, and may be withheld on national security grounds only in the

---

37 See International Mandate-Holders on Freedom of Expression, *2004 Joint Declaration* (6 December 2004), Sub-Section on "Secrecy Legislation", 3rd paragraph; and *op. cit.* footnote 5, Principle 9 (2013 Tshwane Principles).

38 ODIHR, *Guidelines on the Protection of Human Rights Defenders* (2014), par 144.

39 See e.g., OSCE Representative on Freedom of the Media (RFoM), *Access to information by the media in the OSCE region: Trends and Recommendations: Summary of Preliminary Results of the Survey*, 30 April 2007, page 7, which states: *"[t]he definition of state secrets should be limited only to data that directly relate to the national security of the state and where their unauthorized release would have identifiable and serious consequences*"; PACE, Recommendation 1792 (2007) specifically called on the CoE Member States to *"[e]xamine existing legislation on official secrecy and amend it in such a way as to replace vague and overly broad provisions with specific and clear provisions, thus eliminating any risks of abuse or unwarranted prosecutions*"; ODIHR, *Comments on the Draft Law of the Republic of Serbia on Secrecy of Information*, 12 October 2009, par 10.

40 See *op. cit.* footnote 5 (2015 PACE *Resolution 2060 on improving the Protection of Whistle-blowers*).

41 *Op. cit.* footnote 5, Principle 9 (2013 Tshwane Principles).

42 UN Special Rapporteur on the Promotion and the Protection of the Right to Freedom of Opinion and Expression, *Report on the Protection of Sources and Whistleblowers* (2015), A/70/361, par 47; and *op. cit.* footnote 5, Principle 3 (b) (2013 Tshwane Principles).

43 See CCPR, *General Comment no. 34 on Article 19 of the ICCPR, Freedoms of opinion and expression* (2011), par 30; and ibid. par 10 (2015 UN Special Rapporteur on Freedom of Opinion and Expression's Report on Whistleblowers).

44 *Op. cit.* footnote 5, Principles 3 (c) and 4 (2013 Tshwane Principles).

45 *Op. cit.* footnote 5, Sub-Section on "Secrecy Legislation", 3rd paragraph (2004 Joint Declaration); and ibid. Principle 3 (2013 Tshwane Principles).

most exceptional circumstances.[46] There is information about the functioning and activities of intelligence/security services that should always be in the public domain, including the structures and powers of such services, as defined in law; information for evaluating and controlling the use of public funds; the existence and terms of bilateral and multilateral agreements by the state on national security matters; and the overall legal framework for the use of surveillance of all kinds.[47] Furthermore, it is not legitimate to limit disclosure in order to protect against embarrassment or exposure of wrongdoing, violations of international human rights and humanitarian law, maladministration, threats to public health or environmental hazards.[48] Additionally, information should only be classified as a state secret for a definite period of time prescribed by law and there should be clear and transparent procedures to avoid over-classification of documents, including for handling requests for information, regular review mechanisms of classified information and automatic declassification procedures.[49] **The relevant legal framework on access to information and state secrets should be reviewed and amended to provide necessary guidance in line with these standards and the Draft SSU Law should specifically guarantee a right to access to information held by the SSU in line with such standards**.

21. In light of the above, it is welcome that Article 51.3 of the Draft SSU Law provides that it is "*prohibited to impose restrictions on information about the total budget of the Security Service of Ukraine, its competence and functions, as well as instances of unlawful actions on the part of [SSU] personnel*". However, several other provisions of the Draft SSU Law may unduly restrict access to information.

22. Article 12.2 of the Draft SSU Law states that *"[t]he forms, methods and means of exercising powers by the Security Service of Ukraine shall be determined by pertinent legislation, including acts of the Security Service of Ukraine, the content of which may constitute a state secret*". It is no doubt necessary that SSU will be given additional "*secret*" guidance concerning operational aspects, especially in instances where to publish those details would allow potential targets to anticipate or counter them, so rendering them ineffective. At the same time, the *UN SRCT Compilation* expressly recommends that the *"use of subsidiary regulations that are not publicly available is strictly limited, and [that] such regulations are both authorized by and remain within the parameters of publicly available laws",* and should *"not serve as the basis for any activities that restrict human rights"*.[50] Consequently, reliance on them shall not afford

---

[46] *Op. cit.* footnote 5, Principle 10 (2013 Tshwane Principles). For instance, **Latvia**'s Law on State Secrets includes a list of categories of information which have a high presumption of public interest and thus may never be classified (Section 5, 'Information which may not be an Official Secret').

[47] ibid. Principle 10 C and E (2013 Tshwane Principles).

[48] See *op. cit.* footnote 39, page 7 (2007 OSCE RFoM Access to Information by the Media in the OSCE Region); UN Working Group on Arbitrary Detention, *Recommendation: Human Rights and State Secrets*, E/CN.4/2001/14, 20 December 2000, par 90; *UNECE Convention on Access to Information, Public Participation in Decision-Making and Access to Justice in Environmental Matters (Aarhus Convention)*, ratified by Ukraine on 18 November 1999, Article 5 par 1 (c), which imposes a positive obligation on State Parties to immediately disseminate to the public all relevant information held by the government in the event of any imminent threat to human health or the environment. See also Principle 2 (b) of the *Johannesburg Principles on Freedom of Expression and National Security* (1995), adopted on 1 October 1995 by a group of experts in international law, national security, and human rights convened by ARTICLE 19, the International Centre Against Censorship, in collaboration with the Centre for Applied Legal Studies of the University of the Witwatersrand, in Johannesburg and endorsed by the UN Special Rapporteur on Freedom of Opinion and Expression; UN Special Rapporteur on Freedom of Opinion and Expression, *Report on the Protection of Sources and Whistleblowers* (2017), A/70/361, pars 11 and 60; and *op. cit.* footnote 5, Principle 10 (2013 Tshwane Principles). See for instance Romania, Law no 544/2001 on Free Access to Information of Public Interest, Article 13: *"[t]he information that favours or hides the infringement of the law by a public authority or institution cannot be included in the category of classified information and shall be considered as information of public interest.*"

[49] *Op. cit.* footnote 5, Principles 16 and 17 (2013 Tshwane Principles). See also ODIHR, *Guidelines on the Protection of Human Rights Defenders* (2014), par 146; *op. cit.* footnote 39, page 7 (2007 OSCE RFoM Access to Information by the Media in the OSCE Region), which considers that no information should be classified for more than 15 years unless compelling reasons can be shown for withholding it; and NATO Parliamentary Assembly / DCAF, *Joint Study on Parliamentary Access to Classified Information* (2019).).

[50] *Op. cit.* footnote 5, Practice 4 (2010 UN SRCT Compilation).

justification for interfering with human rights.[51] Concerning surveillance in particular, the ECtHR specified that "*the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence*"[52] (see also Sub-Section 5.2 *infra*). Consequently, the use of such SSU "secret" acts should be kept to a minimum and shall not provide a legal basis for interfering with human rights. **To limit the use and effect of such "secret" guidance, Article 12.2 should specify that those are used only "*when strictly necessary*" not to jeopardize the effectiveness of SSU's operation, while specifying that they shall not result in human rights restrictions going beyond what is provided in publicly accessible laws.**[53] **If unpublished guidelines/SSU "secret" acts purport to do so, they should be void and must not be followed by SSU officers, and this should be explicitly stated in the Draft SSU Law**.

23. Article 15.2 of the Draft SSU Law gives the senior management of the SSU the power "*to decline to provide information about the Security Service of Ukraine and its operational activities and/or to make it public, if there are reasonable grounds to believe that providing or disclosing it will pose real or potential threats to Ukraine's state security, human life or health, the environment, or to the security of personnel and operational activities of the Security Service of Ukraine*". This article provides a wide and unchecked margin of discretion to the SSU senior management to limit access to information. **Article 15.2 should be revised to limit such discretion, for instance by including a list of categories of information which shall never be withheld while ensuring that SSU management's power to decline to provide information cannot be invoked when summoned by a court or parliamentary inquiry committee to testify or when other request for information are made by oversight bodies**.

24. Article 51.2 of the Draft SSU Law provides that the SSU "*shall inform the public on its activities through the mass media, its official website, by responding to requests for access to public information and in other forms envisioned by the law, to the extent determined by the Head of the Security Service of Ukraine*". It is welcome that this requires the SSU to both reach out to the public, providing information on its activities of its own accord, and to respond to requests for information from the public. However, **this provision does not determine the terms and respective procedures for access to information, nor does it make reference to a specific access to information law and should be supplemented, also to avoid discretionary prerogatives of the Head of the SSU in that respect**.

25. Finally, several provisions of the Draft SSU Law mention SSU's annual reporting obligations to the President (Article 46.4) and to the Verkhovna Rada (Article 47.5). As per Article 10.4 (10), this falls within the responsibility of the Head of the SSU. There is however **no mention of the content of such reports and it would be advisable to supplement the Draft SSU Law in that respect**. For instance, it is generally considered good practice to publish data regarding the respective representation of women and men, as well as under-represented groups, within the SSU, including at the managerial level, the operation of the intelligence service, including on the use of surveillance measures,[54]

---

[51] See, for example, *Shimovolos v. Russia* (Application no. 30194/09, judgment of 21 June 2011). The ECtHR found that the registration of a human rights activist in a secret surveillance database violated Article 8 of the ECHR. Because the database was created on the basis of an unpublished ministerial order that was not accessible to the public, citizens could not know why certain individuals were registered in the database, what type of information was being stored, how it was being stored, for how long it would be stored, how it would be used, and who would had control over it.

[52] See e.g., ECtHR, *Malone v. United Kingdom* (Application no. 8691/79, judgment of 2 August 1984), par 67.

[53] ibid, par 12.

[54] For instance, information about the number of notification and non-notification of the target(s) of surveillance (when this no longer jeopardizes confidential methods), the number of individuals and the number of communications subject to surveillance each year and

and statistics about complaints and disciplinary cases, and their consequences.[55] **Articles 46-47 of the Draft SSU Law should specify the content of such reports and include these aspects, among others.**

2.4. Protection of Whistle-blowers

26. Articles 14.1 and 15.1 of the Draft SSU Law considerably limit the disclosure of information on the SSU and its operational activities, as well as information obtained or created in the course of SSU's operational activities, which is possible only upon authorization of SSU senior management. Such an approach leaves no room to whistleblowing, which is a key tool to reveal systemic wrongdoing. In the context of security service operation where secrecy generally prevents effective oversight, it is important to ensure the adequate protection of "*whistle-blowers*" (i.e., individuals releasing confidential or secret information although they are under an official or other obligation to maintain confidentiality or secrecy). ODIHR notes with appreciation the recent entry into force of the *Law of Ukraine No. 198-IX "On Amending the Law of Ukraine "On Corruption Prevention" Concerning Whistle-blowers"* dated 17 October 2019. At the same time, the protection of whistle-blowers should not be limited to cases of reporting of corruption or corruption-related offenses but should also cover the reporting of other violations of the law, wrongdoing by public servants, serious threat(s) to health, safety or the environment, or human rights or international humanitarian law violations – all such information being considered presumptively in the public interest.[56] Practice 18 of the *UN SRCT Compilation* recommends as a good practice to put in place "*internal procedures […] for members of intelligence services to report wrongdoing",* together with *"an independent body that has a mandate and access to the necessary information to fully investigate and take action to address wrongdoing when internal procedures have proved inadequate".* Individuals who report wrongdoing should be protected against legal, administrative or employment-related sanctions if they act in "good faith" when releasing information.[57] At least 60 States have adopted some form of whistle-blower protection as a part of their national laws.[58]

27. **Articles 14.4 and 15.1 of the Draft SSU Law should be revised to specifically protect individuals reporting in good faith wrongdoing committed by the SSU or SSU officials, or other matters of significant public concern**. If not provided in other

other aggregate statistics. See *op. cit.* footnote 5, par 137 (2015 Venice Commission's *Report on the Democratic Oversight of the Security Services*); and PACE, *Resolution 2045(2015) on Mass surveillance*, 21 April 2015, par 13. See also *op. cit.* footnote 5, Principle 10.E (2) (2013 Tshwane Principles).

55 For instance, the number of sexual discrimination, harassment, bullying, abuse and other complaints received, as well as the nature of the complaints and their consequences (while not disclosing any details that could identify victims or alleged perpetrators). See e.g., DCAF, *Gender and Complaints Mechanisms - A Handbook for Armed Forces and Ombuds Institutions to Prevent and Respond to Gender-Related Discrimination, Harassment, Bullying and Abuse* (2015), Section 6.3.

56 See International Mandate-Holders on Freedom of Expression, *2004 Joint Declaration* (6 December 2004), Sub-Section on "Secrecy Legislation", 4th paragraph. See also ODIHR, *Guidelines on the Protection of Human Rights Defenders* (2014), par 148; UN Special Rapporteur on freedom of opinion and expression, *Report on the Protection of Sources and Whistleblowers* (2017), A/70/361, pars 10 and 63; and *op. cit.* footnote 5, Principle 37 (2013 Tshwane Principles). See also for reference, PACE, *Resolution 1954 (2013) on National Security and Access to Information*, pars 6 and 9.6..

57 ibid. Sub-Section on "Secrecy Legislation", 4th paragraph (2004 Joint Declaration); and *op. cit.* footnote 5, Practice 18 (2010 UN SRCT Compilation).

58 *Op. cit.* footnote 42, par 27 (2017 UN Special Rapporteur on Freedom of Opinion and Expression's Report on Whistleblowers). See e.g., in Canada (the Canadian Security of Information Act has a special section for persons who are permanently bound by secrecy; the Act outlines specific procedures for the officers of the CSIS to disclose information in the public interest but before disclosing the information, the officer should bring the matter to the attention of Deputy Attorney General, and in case of no response, with the Security Intelligence Review Committee, before disclosing the information (Section 15(5)); Croatia (when an officer receives an unlawful order from superiors, which constitute a criminal act, the person is obliged to notify the chairperson of the Parliamentary Committee and the head of the Office of the National Security Council (Article 67(2) of the SOA Law)); the legal framework in Belgium provides a strong safeguard against executive abuse of powers, by providing the members of the security service with the opportunity to disclose information to the expert oversight body (Committee I), which is mandated to receive complaints and denunciations of individuals who have been *directly concerned by the intervention of an intelligence service*... *Any public officer*, any person performing a public function, and any member of the armed forces directly concerned by the directives, decisions or rules applicable to them, as well as by the methods or actions, may lodge a complaint ... without having to request authorization from his superiors (*Act Governing Review of the Police and Intelligence Services and of the Coordination Unit for Threat Assessment*, Article 40).

legislation, **the Draft SSU Law should explicitly state that the SSU shall prevent retaliation against persons reporting such violations and if they have been dismissed, they should be immediately reinstated or, if they wish so, adequately compensated. It should also define reporting mechanisms and procedures, while including confidentiality clauses to protect the identity of the whistle-blower(s)**.[59] This would be in line with PACE Resolution 2060 adopted in 2015 that called on CoE Member States to "*enact whistle-blower protection laws also covering employees of national security or intelligence services and of private firms working in this field*".[60]

28. In addition, as indicated by the International Mandate-Holders on Freedom of Expression, individuals other than public officials or employees, including journalists and civil society representatives, should never be subject to liability for publishing or further disseminating this information if they do not place anyone in an imminent situation of serious harm, regardless of whether or not it has been leaked to them, unless they committed fraud or another crime to obtain the said information.[61] **This principle should also be adequately reflected in the Draft SSU Law or other relevant legislation pertaining to state secrets.**

3. GENERAL MANDATE OF THE SSU

3.1. Counter-terrorism

29. Various provisions of the Draft Amendments[62] provide the SSU with a very broad and operational mandate for combatting terrorism, financing of terrorism and cyberterrorism.

30. As per the *UN SRCT Compilation*, when counter-terrorism is included in the mandate of security services, states shall "*adopt legislation that provides precise definition of terrorism as well as terrorist groups and activities*".[63] The analysis of the Ukrainian definition of "*terrorism*" and related criminal offences in Articles 258 to 258[5] of the *Criminal Code of Ukraine* goes beyond the scope of this Opinion. At the same time, and while acknowledging that there is no internationally-agreed definition of terrorism,[64] it is important to reiterate that the national legislation shall provide for a clearly and strictly circumscribed definition of "*terrorism*" that is human rights-compliant in accordance with the principles of legal certainty, foreseeability and specificity of criminal law.[65]

---

[59] See e.g., International Labour Organization (ILO), *Law and Practice on Protecting Whistle-blowers in the Public and Financial Services Sectors* (2019), especially pages 6-25.

[60] *Op. cit.* footnote 5, Article 10.1.1 (2015 PACE, *Resolution 2060 on improving the Protection of Whistle-blowers*); and page 31 (2017 EU FRA Surveillance by Intelligence Services). For instance, in France, staff of the intelligence services who witness or observe violations of the intelligence law can address the National Commission for Monitoring of Intelligence Techniques (CNCTR), which can then bring the case before the Council of State and inform the Prime Minister (Interior Security Code, Article L. 861–3).

[61] *Op. cit.* footnote 5, Sub-Section on "Secrecy Legislation", 2nd paragraph (2004 Joint Declaration).. See also ODIHR, *Guidelines on the Protection of Human Rights Defenders* (2014), pars 146 and 149, which states that *"[t]he sharing and publication of otherwise publicly available information or academic research should not be viewed as unlawful disclosure of state secrets, even when their disclosure into the public domain occurred in violation of secrecy laws*".

[62] E.g., Articles 2 par 2 (2), Articles 6 par 4, Article 12 par 1 (8), (11) and (12) and Article 17 of the Draft SSU Law and amended Article 19 of the Law "On National Security of Ukraine".

[63] *Op. cit.* footnote 5, Practice 2 and par 10 (2010 UN SRCT Compilation).

[64] UN Special Rapporteur on counter-terrorism, *2005 Report*, UN Doc. E/CN.4/2006/98, pars 26-28; *2010 Report on Ten areas of best practices in countering terrorism*, UN Doc. A/HRC/16/51 (2010), pars 26-28; and 2019 *Report to the UN Commission on Human Rights*, UN Doc. A/HRC/40/52, 1 March 2019, par 19.

[65] This requires that criminal offences and related penalties be defined clearly and precisely, so that an individual knows from the wording of the relevant criminal provision which acts will make him/her criminally liable. In that respect, the UN Special Rapporteur on counter-terrorism has noted that any definition of terrorism would require three cumulative elements to be human rights-compliant i.e., it should amount to an action: (1) corresponding to an offence under the universal terrorism-related conventions (or, in the alternative, action corresponding to all elements of a serious crime defined by national law); and (2) done *with the intention* of provoking terror or compelling a government or international organization to do or abstain from doing something; and (3) passing a certain threshold of seriousness, i.e., either (a) amounting to the intentional taking of hostages, or (b) intended to cause death or serious bodily injury, or (c) involving lethal or serious physical violence. See UN Special Rapporteur on counter-terrorism, *2010 Report*, A/HRC/16/51, 22 December 2010, par 27; *2019 Report*, par 75 (c); and *UN Security Council Resolution 1566 (2004)*, S/RES/1566 (2004), par 3. See also OSCE TNTD-SMPU and ODIHR *Preventing Terrorism and Countering VERLT* (2014), pages 27-30; and ODIHR, *Guidelines on Addressing the Threats and Challenges of "Foreign Terrorist Fighters"* (2018), Chapter 3.1.

From a cursory review of Article 258 of the Criminal Code of Ukraine, the constitutive elements of the offence of terrorism do not seem to comply with international recommendations, especially as it includes vague terms such as "*other acts that […] cause significant property damage or other serious consequences*" and the *mens rea*[66] is not limited to the intention of "*provoking terror or compelling a government or international organization to do or abstain from doing something*". It is worth emphasizing that the UN Special Rapporteur on counter-terrorism has also expressly stated that "*[d]amage to property, absent other qualifications, must not be construed as terrorism*".[67] **It is thus recommended to review the definition of terrorism and related criminal offences of the Criminal Code to ensure greater compliance with international human rights standards and recommendations**.

31. Overall, the SSU would be in charge of preventing terrorism, conducting comprehensive targeted and strategic surveillance regarding potential terrorists, conducting anti-terrorist operations on the ground both in Ukraine and non-government-controlled areas, and carrying out detective operations, pre-trial investigations related to terrorism charges. In democratic societies, such tasks are generally distributed across foreign and domestic security services (conducting surveillance), specialized anti-terror units in national police (conducting operations) and investigation departments of the police and prosecutorial/judicial authorities (conducting and overseeing pre-trial investigation). This prevents the consolidation of intelligence, police and prosecutorial/judicial powers in one single entity as well as allows for better checks and balances and oversight. If the SSU retains countering-terrorism as part of its mandate, **it should be limited to collecting, processing and sharing information on terrorist groups and activities, both of which should be narrowly defined by publicly accessible laws. The SSU's mandate should not include the power to carry out anti-terrorist operations on the ground, to conduct detective operations and respective investigations concerning terrorism. These powers should be divided between different competent law enforcement and other public authorities.**

32. In that respect, Article 6.4 of the Draft SSU Law refers to an Anti-Terrorism Centre, operating under the SSU. The Centre is not only mandated to organize/coordinate counter-terrorism efforts but also to *directly conduct anti-terrorism operations* on the ground. This indicates a strong law enforcement mandate, including potential use of force (see Sub-Section 5 *infra*). As per international recommendations, **the Anti-Terrorism Centre of the SSU should be mainly tasked with collecting, processing and sharing intelligence on terrorism-related issues, and their operational/law enforcement mandate should be limited to the extent possible**.[68]

33. Article 12.8 of the Draft SSU Law empowers the SSU to "*take measures aiming to combat terrorism and financing of terrorism, to prevent and terminate activities of international terrorist organisations in the territory of Ukraine*". **To avoid abuse, it is important to define the list of international terrorist organizations, as recognized by Ukraine, in a publicly available law promulgated by the Parliament**. If the authorities are contemplating to use as a reference the list of "*terrorist organizations*" designated by international or regional organizations, this may limit the scope for abuse though not entirely since such listing processes have been criticized for their lack of legal certainty,

---

66 Article 258 of the Criminal Code of Ukraine refers to acts committed "*to violate public safety, intimidate the population, provoke military conflict, international complication, or in order to influence decisions or acts or omissions of public authorities or local governments, officials of these bodies, associations of citizens, legal entities, international organizations, or to draw public attention to certain political, religious or other views of the perpetrator (terrorist)*".

67 ibid. par 75(c) (2019 Report of the UN Special Rapporteur on counter-terrorism).

68 *Op. cit.* footnote 5, Practices 1 and 2 (2010 UN SRCT Compilation).

arbitrariness, politicization, procedural inadequacies and due process deficiencies.[69] Accordingly, if this is the option chosen by Ukraine, there must be access to domestic judicial review of any domestic implementing measures pertaining to persons on such list and adequate minimum safeguards must be in place, in line with international recommendations.[70]

34. Article 12.1 (11) of the Draft SSU Law specifically refers to the "*prevention and suppression of operation, in the territory of Ukraine, of illegal armed and paramilitary forces, other groups or formations whose activities pose a threat to state security*". Such a wording is overly vague and broad and may result in arbitrary expansion of SSU's mandate if threats to national security are not strictly defined by law. This broad terminology cannot exclude that this may lead to abuse against political opposition or certain associations that defend positions or carry out legitimate activities that may "*offend, shock or disturb*" the State or any part of the population.[71] As stated in the OSCE/ODIHR-Venice Commission *Guidelines on Freedom of Association*, the rights to freedom of expression and to freedom of association entitle associations to pursue objectives or conduct activities that are not always congruent with the opinions and beliefs of the majority or run precisely counter to them.[72] This includes e.g., "*imparting information or ideas contesting the established order or advocating for a peaceful change of the Constitution or legislation by, for example, […] asserting a minority consciousness, […] calling for regional autonomy, or even requesting secession of part of the country's territory*".[73] **To avoid any risk of abuse, the wording "*other groups or formations whose activities pose a threat to national security*" should be removed from Article 12.1 (11) of the Draft SSU Law or defined more precisely, especially as regards the nature of the threat that organizations or groups may pose.**

35. As it stands, the Draft SSU Law refers to the "*preventing, detecting and terminating crimes against state security, peace and human safety*" and "*other crimes posing a threat to state security*" (Article 2.2 (4)). Beyond the overbroad and imprecise definition of "*state security*", it is unclear which crimes this would cover. Sections I and IX of the Special Part of the Criminal Code of Ukraine cover crimes against the "fundamental of national security of Ukraine" and against "public security",[74] while crimes against peace,

---

[69] UN Special Rapporteur on counter-terrorism, *Report on compliance by the United Nations with international human rights law while countering terrorism*, UN Doc. A/65/258 (2010), pars 55-58. See also e.g., ECtHR, *Nada v. Switzerland* [GC] (Application no. 10593/08, judgment of 12 September 2012); Al-Dulimi and Montana Management Inc. v. Switzerland (Application no. 5809/08, judgment of 21 June 2016); and CCPR, *Sayadi & Vinck v. Belgium*, Views adopted on 22 October 2008, UN Doc. CCPR/C/94/D/1472/2006.See also e.g., ODIHR, *Guidelines on Addressing the Threats and Challenges of "Foreign Terrorist Fighters"* (2018), pages 22-23; Venice Commission, *Opinion on the Law on Preventing and Combatting Terrorism of Moldova*, 22 October 2018, par 75 ; and PACE, *Resolution 1597 (2008) on United Nations Security Council and European Union blacklists*.

[70] In addition to judicial review, the UN Special Rapporteur has identified six minimum safeguards with regard to the implementation of any sanctions against individuals or entities on any terrorist list: (1) sanctions against an individual or entity, including the terrorist listing, shall be based on reasonable grounds to believe that the individual or entity has knowingly carried out, participated in or facilitated a terrorist act, as properly defined; (2) the listed individual or entity shall be promptly informed of the listing and its factual grounds, the consequences of such listing, and the rights pertaining to the listing (i.e. the guarantees identified in subparagraphs (3) to (6) of this paragraph); (3) the listed individual or entity shall have the right to apply for delisting or non-implementation of the sanctions, and shall have a right to a judicial review of the decision resulting from the application for delisting or non-implementation, with due process applying to such review, including disclosure of the case against the person and such rules concerning the burden of proof that are commensurate with the severity of the sanctions; (4) the listed individual or entity shall have the right to make a fresh application for delisting or lifting of sanctions in the event of a material change of circumstances or the emergence of new evidence relevant to the listing; (5) the listing of an individual or entity, and the sanctions resulting from it, shall lapse automatically after 12 months, unless renewed through a determination that meets the guarantees in subparagraphs (1) to (3) of this paragraph; and (6) compensation shall be available for persons and entities wrongly affected, including third parties – see UN Special Rapporteur on counter-terrorism, *2010 Report on Ten areas of best practices in countering terrorism*, UN Doc. A/HRC/16/51 (2010), Practice 9.

[71] UN Special Rapporteur on counter-terrorism, *2015 Thematic Report*, A/HRC/31/65, 22 February 2016,

[72] ODIHR-Venice Commission, *Guidelines on Freedom of Association* (2015), par 182.

[73] ODIHR-Venice Commission, *Guidelines on Freedom of Association* (2015), par 182.

[74] These include for Section I: Article 109 (Actions aimed at forceful change or overthrow of the constitutional order or take-over of government) and financing of such actions (Article 110^2), Article 110 (Encroachment on the territorial integrity and inviolability of Ukraine), Article 111 (High Treason), Article 112 (Encroachment on the life of a state or public figure), Article 113 (Sabotage), Article 114 (Espionage) and Article 114^1 (Obstruction of lawful activity of the Armed Forces of Ukraine and other military formations); and for Section IX various criminal offences including in relation to organized crimes, banditry, terrorism and related offences, firearms, ammunition, explosives or radioactive materials, etc.

security of mankind and international legal orders and crimes against public safety are covered by Sections XX and IX respectively, but it is not clear whether other criminal offences would be potentially covered too. Given the broad wording, this seems to imply that the SSU could potentially be involved in the investigation of almost any crime. **It is recommended to specify more clearly and narrowly the nature of the criminal offences for which the SSU would have investigating and law enforcement powers – if retained at all, for instance by including a cross-reference to the relevant sections of the Criminal Code, providing that such offences pose a threat to national security**.

3.2. Organized Crimes

36. Article 12.1 (9) and (10) gives extensive intelligence and law enforcement powers to the SSU to combat organized crimes. Article 18.3 of the Draft SSU Law requires compliance with the *Law of Ukraine "On Organisational and Legal Principles of Combating Organised Crime"* while the last Section on Final and Transitional Provisions amends the said Law and gives the SSU a main role in preventing and combatting organized crimes. As emphasized in the *ODIHR Opinion on the Draft Concept*, the SSU should generally not be involved in the fight against organized crimes, unless these pose a clear and present danger to national security.[75] If this competence is retained at all, **this caveat should be expressly mentioned in the Draft Amendments whenever references to such criminal offences are made**. Moreover, **Article 12.1 (9) and (10) should be strictly limited to the collection, analysis and sharing of information on such organized crimes thus focusing exclusively on intelligence collection, and not on the actual investigation of such crimes**.

37. More specifically, Article 12.1 (10) allows the SSU to combat illicit trafficking in narcotic drugs, which is not in line with the case law of the ECtHR which does not recognize simple "*involvement in drug trafficking"* as a threat to national security.[76] **This competence should be reconsidered entirely as such crimes should rather be left to the National Police's competence**.

3.3. Combatting Corruption

38. Article 12.1 (18) and (37) provides the SSU with a broad anti-corruption mandate, whether or not such acts are linked to threats to national security. Article 12.1 (18) of the Draft SSU Law tasks the SSU with surveilling, detecting and investigating "*unduly gained assets*", which is considered as an act associated with economic crimes and corruption.[77] "Economic objectives" could potentially fall within the SSU's mandate but only if they present a clear and present danger to national security'.[78] The Venice Commission has specified the kind of economic crimes that may legitimately require conducting intelligence activities to protect national security, which would generally be limited to the "*proliferation of weapons of mass destruction, circumvention of UN/EU sanctions, and major money laundering"*.[79] Of note, Article 36 of the *UN Convention against Corruption* calls for establishing "specialised authorities" for combatting corruption "through law enforcement",[80] thus underlining the importance of separate, independent body with exclusive mandate to counter corruption, instead of incorporating anti-corruption mandate into domestic security services, as contemplated in the Draft

---

75 See e.g., *op. cit.* footnote 5, par A.2 (1999 PACE Recommendation 1402).
76 See e.g., ECtHR, *C.G. and others v. Bulgaria* (Application no. 1365/07, judgment of 24 April 2008), pars 40-43.
77 See UN Convention against Corruption Article 20 (Illicit Enrichment), <https://www.unodc.org/unodc/en/treaties/CAC/>.
78 *Op. cit.* footnote 5, par A.2 (1999 PACE Recommendation 1402).
79 *Op. cit.* footnote 5, par 10 (2015 Venice Commission's *Report on the Democratic oversight of Signals Intelligence Agencies*). ,*Report on the Democratic oversight of Signals Intelligence Agencies*
80 *UN Convention against Corruption*, adopted by the UN General Assembly on 31 October 2003. Ukraine ratified this Convention on 2 December 2009.

SSU Law. Giving the SSU such a broad anti-corruption mandate would also result in overlapping mandates with the dedicated agency "National Anti-corruption Bureau of Ukraine" (NABU) or with law enforcement agencies authorized with investigation of corruption-related crimes.

39. In light of the above, **the SSU's broad anti-corruption mandate should be removed entirely, or at a minimum limited to cases relating to the proliferation of weapons of mass destruction, circumvention of UN/EU sanctions, and major money laundering, which are clearly linked to national security threats.**

3.4. Border and Migration Management

40. Article 12.1 (24) of the Draft SSU Law gives the SSU broad border enforcement and migration management powers. In the field of migration management, the SSU is tasked with "*development and implementation of measures related to individuals' entry to and departure from Ukraine, foreigners and stateless persons' stay in its territory"*. These are typical migration management tasks, which should generally fall under the purview of border police and civilian migration authorities. Indeed, civilian authorities are better positioned to conduct administrative procedures relating to entry, residence and exit, come into regular contact with migrants and asylum seekers and operate with a greater degree of transparency and judicial scrutiny on administrative acts and decisions. Giving these powers to domestic security services with broad surveillance/intelligence and law enforcement powers such as the SSU is problematic first because they generally operate in an environment largely characterized by secrecy and clandestine powers. This could increase the risk of unlawful enforced returns and denial of the right to seek asylum or other forms of protection without effective right to appeal. There are numerous ECtHR judgements concerning the involvement of security/intelligence agencies engaging in secret rendition operations.[81] This may constitute a threat to the fulfilment of fundamental human rights and principles of international law, such as the right to seek asylum, principles of non-refoulement and prohibition of collective expulsion, as stipulated in the UN Convention Against Torture[82] and Protocol no. 4 to the ECHR[83] respectively. Moreover, giving migration and border management-related tasks to the SSU may create duplication and overlap of mandates with the State Migration Service of Ukraine and the State Border Guard Service, thus creating confusion regarding the respective roles and responsibilities of such entities, and potential gaps in the execution of tasks as well as their oversight.

41. Hence, **SSU's mandate should be revised with a view to remove any task allowing SSU's active involvement in the implementation of border and migration management-related activities. SSU's involvement can only be justified in conducting lawful surveillance on individuals who are deemed to constitute a threat to national security**, such as suspected "foreign terrorist fighters". However, this would fall under SSU's mandate on countering terrorism, therefore questioning the need for a separate border and migration management mandate.

3.5. Cybercrimes

42. Regarding cybercrimes, it is welcome that Article 12.1 (14) specifically seeks to limit SSU's competence to "*cybercrime, the consequences of which could jeopardise vital*

---

81 See, for instance, ECtHR, *El Masri v. The Former Yugoslav Republic of Macedonia* [GC] (Application no. 39630/09, judgment of 13 December 2012).

82 Article 3 of the *UN Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment*, which was ratified by Ukraine on 24 February 1987.

83 The *Protocol no. 4 to the ECHR* was ratified by Ukraine on 11 September 1997.

interests of the State". However, "vital interests of the State" are not defined elsewhere in the Draft SSU Law nor in the Law on National Security of Ukraine. **It is recommended to define such a term**. It is also welcome that "cybersecurity" is included as part of the SSU's mandate (Article 2.2 (3) of the Draft SSU Law). At the same time, it is not clear what SSU's role would be in that respect as this is not further detailed in the Draft SSU Law. It is true that Article 8.2 (3) of the *2017 Law of Ukraine on the Basic Principles of Cybersecurity* details the functions of the SSU in relation to cybersecurity[84] and **it would be useful to make a cross-reference to such legislation to clarify SSU's role in that respect**.

3.6. Administrative Offences

43. Article 12.1 (19) of the Draft SSU Law appears to give the SSU the power to handle administrative offences that are referred to the SSU "*under applicable law*". Generally, administrative responsibility applies to behaviours encroaching on public order, property, the rights and freedoms of citizens, if these violations by their nature do not trigger criminal liability (Article 9 of the *Code of Ukraine on Administrative Offences*). Therefore, such administrative offences are generally not considered to reach a threshold of seriousness and endanger public order justifying to be criminalized, and as such should not fall within the SSU's mandate to protect from national security threats. **The drafters should remove such a power from the Article 12.1 (19) of the Draft SSU Law.**

4. ORGANIZATION OF THE SSU

4.1. Head of the SSU

44. According to Article 10.2 of the Draft SSU Law, the Head of the SSU is appointed and dismissed by the Verkhovna Rada of Ukraine upon the recommendation of the President of Ukraine and is appointed for a term of office of six years. Hence, the Head of the SSU's term of office is different from the President five years' term of office, which should in principle reduce the potential risk of politicization of the position. **It is not clear whether this term of office is renewable or not and this should be clarified.**

45. Article 10.3 of the Draft SSU Law lists the eligibility criteria for appointment to the position of Head of the SSU as well as the grounds that make a candidate ineligible for the position, also referring to restrictions set forth in Article 23 for SSU personnel (see below). Especially, Article 10.3 (3) specifies that "*previous stay outside of Ukraine for three years*" renders a candidate ineligible. Such a restriction is rather unusual and may arbitrarily prevent a person's nomination for the position whereas this is not necessarily and directly linked to potential risks to national security and should not as such automatically disqualify a nominee. **Such a provision should be reconsidered**.

46. The Draft SSU Law fails to further detail the appointment procedure, whereas this is key to protect against political interference. While there is no single prescriptive international standard stipulating how heads of security services should be appointed, there is a number of country good practices suggesting that nomination or appointment procedures should not be left to the sole discretion of the executive, should be based on publicly available

[84] Article 8 par 2 (3) of the *2017 Law of Ukraine on the Basic Principles of Cybersecurity* states that the SSU "*prevents, detects, stops and discloses crimes against peace and security of mankind committed in cyberspace; carries out counterintelligence and operative-search measures aimed at combating cyberterrorism and cyber espionage, secretly checks the readiness of critical infrastructure facilities for possible cyber attacks and cyber incidents; counteracts cybercrime, the consequences of which may threaten the vital interests of the state; investigates cyber incidents and cyberattacks on state electronic information resources, information, the protection of which is established by law, critical information infrastructure; provides response to cyber incidents in the field of state security*".

laws and clear and objective criteria, and should include some form of consultation with the Parliament ensuring broad political backing or other scrutiny from outside the executive, while ensuring that the process is transparent and merit-based.[85] This could also be done by ensuring that the vacancy notice is widely published to ensure a variety of applications, as well as that the Verkhovna Rada holds a public hearing with potential candidate(s), clearly stating that the modalities for selection and appointment should be non-discriminatory and gender-sensitive, while ensuring that the final appointment is supported by wide consensus, for example by requiring a qualified majority to ensure support from minority parties.[86] **The legal drafters should provide more detailed appointment procedure with the objective to ensure greater openness, transparency and merit-based selection process.**

47. Legal grounds for the dismissal of the Head of the SSU should be clearly stipulated by law to prevent arbitrariness. Article 10.10 of the Draft SSU Law enumerates such grounds, which is welcome. However, Article 10.10 (5) refers to the "*systematic failure to perform their official duties*" or showing "*inaptitude*" for the position held, which is rather vague and could potentially be utilized as a ground for SSU Head's arbitrary dismissal or threat thereof. **Such a wording should be revised to specify such ground in order to avoid potential arbitrariness.**

4.2. Civil Direction and Control of the SSU

48. Article 2.4 of the Draft SSU Law states that the SSU "*is subordinate to the President of Ukraine and controlled by the Verkhovna Rada of Ukraine*". In general, the Draft SSU Law fulfils the OSCE commitments for civil control of the SSU.[87] At the same time, the Draft SSU Law still envisages the SSU as a military institution. As emphasized in Sub-Section 3.5 of the *Opinion on the Draft Concept*, it is essential that **the Draft SSU Law explicitly defines the SSU as a civilian institution**.

49. Moreover, security services should not be politicized nor used as instruments against opponents by a ruling party or incumbent heads of state. It is thus essential to maintain impartiality of intelligence, create effective structures shielding intelligence reporting from policy bias and prevailing political concerns, and maintain sufficient independence to flag new and emerging threats that fall outside the view of established institutional and policy perspectives. It is therefore essential that **the Draft SSU Law clarifies the SSU's relationship with the President of Ukraine and with the Verkhovna Rada**, to limit the risk of the SSU being used for inappropriate political purposes. As stated in the *ODIHR Opinion on the Draft Concept*, it may be advisable to provide for control and

---

[85] *Op. cit.* footnote 5, par 19 (2010 UN SRCT Compilation). See also Venice Commission-CoE Directorate of Human Rights (DGI), *Joint Opinion on the Draft Law no. 281 Amending and Completing Moldovan Legislation on the So-Called "Mandate of Security"*, CDL-AD(2017)009, par 53. In a number of European states, to ensure that the head of the intelligence agency has a broad political backing, the competent parliamentary committees hold a hearing with a nominee and can issue a non-binding opinion or recommendation on the proposed appointment (e.g., in Estonia, Portugal, Hungary, and Croatia - see e.g., *op. cit.* footnote 5, pages 107-108 (2011 European Parliament's *Study on the Parliamentary Oversight of Security and Intelligence Agencies in the EU*). For instance, in Croatia, the Director of the security service (SOA) is appointed by a decision co-signed by the President and the Prime Minister, for a four-year term, with possibility for renewal; the law additionally requires that the opinion of the Parliamentary Committee for Interior Policy and National Security is obtained (Article 66 (1) of the *Act on the Security and Intelligence System of the Republic of Croatia*); while the parliamentary committee does not have a formal veto power, a strongly articulated negative opinion of a candidate would damage the legitimacy of the President's and the PM's nomination. In Canada, the director of the intelligence agency is appointed for a five-year term, renewable only once, by the cabinet through a process known in Canada as Governor in Council (GIC) appointment, which is open to all Canadians, transparent and merit-based (see Canada, Security of Information Act (R.S.C., 1985, c. O-5), Section 4).

[86] ibid.

[87] The *OSCE Moscow Document* (1991), OSCE participating States committed to ensure that their security agencies, including intelligence services "*are subject to the effective direction and control of the appropriate civil authorities*". In other words, security agencies should be directed by civil authorities with a constitutional mandate and democratic legitimacy.

supervision by a civilian authority other than the head of state or of government, as recommended by the PACE.[88]

50. Another way to limit the potential politicization of the SSU is to include provisions in the Draft SSU Law explicitly **prohibiting SSU from targeting lawful activities of political parties, NGOs, national minorities, religious or belief groups or other particular groups of the population** (see also recommendations concerning specific SSU powers under Sub-Section 5 *infra*).

5. POWERS OF THE SSU

51. Article 12 of the Draft SSU Law provides a very extensive list of forty-three "powers" of the SSU. While it is welcome to describe in details the nature of the SSU's powers, the said powers seem to extend far beyond the normal powers granted to security services in other European countries. They at times include vague and open-ended provisions. Moreover, a number of the more intrusive powers lack the *ex ante* and *ex post facto* safeguards that would be expected under international human rights law and according to good practices. **It would be useful to separate those powers that are especially intrusive of human rights** (especially law enforcement powers, e.g., pre-trial investigation, covert measures of surveillance, use of force, search and seizure, arrest and detentions), **which should apply only in relation to criminal offences that present a clear and present danger to national security and be accompanied by additional, more stringent, safeguards**. This will also ensure that those intrusive powers are not used for more general tasks of the SSU.

52. An overall concern is that many of the provisions of the Draft SSU Law mirror the overt and covert investigative actions provided for in the Criminal Procedure Code (CPC), but without specifying the procedural safeguards and guarantees provided in the CPC, nor expressly stating that the SSU should comply with the CPC when carrying out such actions. As emphasized in *ODIHR Opinion on the Draft Concept*, the exercise of law enforcement powers by the SSU, if retained at all, should be subject to the same legal safeguards and oversight that apply to other law enforcement agencies.[89] Moreover, the CPC provides detailed rules concerning the conduct of various forms of secret surveillance, distinguishing for instance those carried out in public space from those in private places (the latter being more intrusive), and providing other special conditions that overt or covert detective activities must comply with in order to ensure compliance with the human rights of those affected by them. While Article 38 of the CPC refers to security bodies/authorities as entities which may carry out pre-trial investigations, **it is recommended to explicitly spell out in the Draft SSU Law that the respective SSU operations shall be carried out in full compliance with the requirements of the CPC, whenever relevant, with specific references to the relevant provisions of the CPC**.

53. The following sections will not go over each and every one of the powers but will emphasize those which may potentially unduly impact on human rights and fundamental freedoms and which should therefore be accompanied by strong safeguards.

---

[88] *Op. cit.* footnote 5, par C.1 (1999 PACE Recommendation 1402), which states that *"[o]ne minister should be assigned the political responsibility for controlling and supervising internal security services, and his[/her] office should have full access in order to make possible effective day-to-day control. The minister should address an annual report to parliament on the activities of internal security services*".

[89] *Op. cit.* footnote 5, Practice 28 (2010 UN SRCT Compilation).

5.1. Pre-trial Investigation of Criminal Offences

54. Article 12.1 (17) of the Draft SSU Law refers to the power to carry out pre-trial investigation of "*criminal offenses falling within the investigative jurisdiction of security agencies*" and to "*take measures to enable criminal proceedings as required by law*". As mentioned in par 35 *supra*, the category of criminal offences falling within the SSU's mandate is not entirely clear. If retained at all, **pre-trial investigation powers of the SSU should not encompass the entire mandate of the SSU but instead be limited to specific national security threats, such as terrorism**.[90] **Article 12.1 (17) should also only cover the type of criminal offences that fall (exclusively) within the competence of the SSU and not other "*security agencies*"**.

55. The Final and Transitional Provisions would amend Article 216 of the Criminal Procedure Code, which would read: "*[t]he Prosecutor General or their authorised Deputy, upon request of the Head of the [SSU] or their Deputy, may resolve to transfer criminal proceedings regarding crimes, referred to in part one and parts three through five of this Article, to the investigative jurisdiction of the investigating security agencies, if the respective crime poses a threat to the state security of Ukraine".* Such a provision places the SSU above the prosecutorial authorities, by giving the power to the Head of the SSU to order a prosecutor to drop the investigation of a case. This provision, read in conjunction with Article 21, which makes all demands of SSU legally binding on all public authorities, does not leave any room for rejecting the SSU's request for taking over a case. This may also potentially block independent investigation of allegations relating to the SSU itself, or its personnel. **This prerogative should simply be removed from Article 216 of the Criminal Procedure Code.**

5.2. Covert Measures/Surveillance

56. Article 3.1 (3) of the Draft SSU Law provides that the SSU shall carry "*detective operations*" and several sub-paragraphs of Article 12 on SSU powers refer to such operations (sub-paragraphs (7), (20), (21), (34) and (39)). It is understood from Article 2 of the *Law of Ukraine "On Detective Operations"* that "detective operations" mean "*a system of overt and covert search, reconnaissance and counterintelligence activities carried out with the use of operational and operational-technical means*". Moreover, various sub-paragraphs under Article 12.1 give the SSU an overall surveillance mandate, such as sub-paragraphs (6), (15) (supporting strategic communications system), (20)-(22) (covert information gathering and interception of telecommunications), and (25)-(26) (use of undercover agents). Article 13 regulates in further details the information collection procedures.

57. The ECtHR has accepted that "*the existence of some legislation granting powers of secret surveillance over the mail, post and telecommunications is, under exceptional conditions, necessary in a democratic society in the interests of national security and/or for the prevention of disorder or crime*".[91] At the same time, the ECtHR also emphasized that *"[i]n view of the risk of abuse intrinsic to any system of secret surveillance, such measures must be based on a law that is particularly precise*" and that *"[i]t is essential to have clear, detailed rules on the subject*".[92]

58. The state acquisition and recording of information on individuals obtained through surveillance, interception of communication or undercover operations are highly intrusive

---

[90] *Op. cit.* footnote 5, par 41 (2010 UN SRCT Compilation).
[91] See e.g., ECtHR, *Klass and Others v. Germany* (Application no. 5029/71, judgment of 1978), par 48.
[92] See e.g., ECtHR, *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria* (Application no. 62540/00, judgment 28 June 2007), par 75.

and, if abused, lead to serious human rights violations, in particular of the right to respect for private and family life enshrined in Article 17 of the ICCPR and Article 8 of the ECHR. It is therefore important that such surveillance activities pursue a legitimate aim and are carried out with due regard to the principles of legality, necessity and proportionality, while being subject to judicial control, and that the state ensures the utmost transparency about the legal basis, scope and modalities of such measures and methods.[93] Moreover, such powers shall, in light of their intrusive character, the lack of public scrutiny and the ensuing risk of misuse, be subject to extremely strict conditions and safeguards,[94] including effective *ex ante* judicial authorization.[95] This is with due consideration of these principles that the Draft SSU Law and subsequent by-laws on surveillance should be drafted.

5.2.1. Targeted Surveillance

59. Article 12.1 (20) authorizes the SSU to use technical means for covert search, monitoring, selection, recording and processing of information in the course of detective and counterintelligence operations as well as criminal proceedings, thus allowing targeted secret surveillance measures. When assessing the necessity of the surveillance, the ECtHR looks for "*adequate and effective guarantees against abuse*"[96]. This assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law.[97] The ECtHR has set "*minimum safeguards against abuse*" when authorities are resorting to such measures. Accordingly, a statutory law should clearly define the conditions and circumstances in which the authorities are empowered to resort to such measures, including:

    (i) the nature of the offences in relation to which secret surveillance may be ordered;[98]

    (ii) the definition of the categories of people who may be placed under surveillance;

    (iii) the limits on the duration of the surveillance;

    (iv) the procedure to be followed for examining, protecting, using and storing the data obtained;

    (v) the precautions to be taken when communicating the data to other parties; and

    (vi) the circumstances in which the intercepted data may or must be erased or destroyed.[99]

60. Furthermore, the legislation should also specify the permissible objectives of intelligence collection; the threshold of suspicion required to initiate (or continue) surveillance measures (there should be concrete facts indicating the criminal offence/security-

---

93 See UN Special Rapporteur on freedom of opinion and expression, *2013 Report*, pars 91-92, which notes how important it is for States to be transparent about the use and scope of communications surveillance techniques and powers, particularly in relation to internet service providers. See also *op. cit.* footnote 5, Principle 10.E (2013 Tshwane Principles).

94 See ECtHR, *Uzun v. Germany* (Application no. 35623/05, judgment of 2 September 2010), par 63.

95 See e.g., ECtHR, *Solska and Rybicka v. Poland* (Application nos. 30491/17 and 31083/17, judgment of 20 September 2018), pars 109-112; and *Weber and Saravia v. Germany* (Application no. 54934/00, judgment of 29 June 2006), par 106.

96 See especially ECtHR, *Roman Zakharov v. Russia* [GC] (Application no. 47143/06, judgment of 5 December 2015), pars 232 and 236.

97 See e.g., ECtHR, *Klass and Others v. Germany* (Application no. 5029/71, judgment of 1978), pars 49-50. See also ibid. par 232 (2015 ECtHR [GC] *Roman Zakharov v. Russia* [GC]).]).

98 The ECtHR does not necessarily require to exhaustively list, by name, the specific offences, but sufficient details should be provided on the nature of the said offences; see ECtHR, *Roman Zakharov v. Russia* [GC] (Application no. 47143/06, judgment of 5 December 2015), pars 243-244.

99 See e.g., ECtHR, *Weber and Saravia v. Germany* (Application no. 54934/00, decision of 29 June 2006), par 95; and *Zakharov v. Russia* [GC] (Application no. 47143/06, judgment of 3 December 2015), par 231. See also *op. cit.* footnote 5, Practice 21 (2010 UN SRCT Compilation); and Principle 10.E (2013 Tshwane Principles)..

threatening conduct and a "*probable cause*", "*reasonable suspicion*" or other similar requirement that a person, or persons, have committed, are committing, or are planning the commission of a security offence);[100] clearly define their scope, including the types of personal data that may be collected and/or processed for national security purposes; identify the authorities competent to authorize, review and carry out such measures; and determine the rules governing the use of evidence in potential criminal cases.[101] It is also important that such special operational and investigative actions not be used to obtain confidential or privileged communications, such as those involving a defence counsel,[102] a priest (and related secret confession and/or religious affiliation), doctor/psychologist or psychiatrist's patients' files/medical records.[103] Moreover, the right of journalists to protect the confidentiality of their sources, widely recognised by international bodies,[104] should also be safeguarded. In view of the fact that the media plays a crucial role in any society, some States have instituted specific measures to protect journalists from being targeted by intelligence services.[105]

61. **It is important that these principles be reflected in the Draft SSU Law, or where appropriate, in other relevant legislation to which the Draft SSU Law should make a cross-reference**. Moreover, and as done in some countries, **the Draft SSU Law could explicitly prohibit intelligence services from using their powers to target lawful political activity or other lawful manifestations of the rights to freedom of association, peaceful assembly and expression**.[106]

62. One additional safeguard is the requirement that the agencies must be subject to an external oversight ensuring that the legal preconditions for use of its powers, such as interception, bugging and video surveillance, are met.[107] In most European countries, this external person/entity is a judge and the ECtHR has expressed a clear preference for a system of judicial control, stating that it offers "*the best guarantees of independence, impartiality and a proper procedure*"[108] (see also Sub-Section 6.3 *infra* on judicial oversight). A further safeguard is *post hoc* remedies against security agencies for violations of rights.[109] **It recommended that the Draft SSU Law explicitly provides that such surveillance be subject to *ex ante* judicial authorization, but also ongoing oversight of information collection measures (supervision of investigations, ordering the termination of surveillance and ordering the destruction of data collected) and ex-post adjudication of cases** (see also Sub-Section 6.3 *infra* on judicial oversight).

---

100 See e.g., *op. cit.* footnote 5, par 38 (2015 Venice Commission *Report on the Democratic Oversight of Signals Intelligence Agencies).*

101 See *op. cit.* footnote 5, Principle 10.E (2013 Tshwane Principles). See also e.g., ECtHR, *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria* (Application no. 62540/00, judgment of 28 June 2007), pars 76-77; ECtHR, *Uzun v. Germany* (Application no. 35623/05, judgment of 2 September 2010), par 63. See also *op. cit.* footnote 5, Practice 21 (2010 UN SRCT Compilation).

102 See e.g., ECtHR, *Kopp v. Switzerland* (Application no. 23224/94, 25 March 1998), where the Court emphasized that legally privilege communications between a lawyer and his or her client require better protection from interception than delegation of the decision about recording to a junior clerk.

103 See e.g., *op. cit.* footnote 5, par 101 (2015 Venice Commission *Report on the Democratic Oversight of Signals Intelligence Agencies).*

104 See par 40 of the *1986 Document on the OSCE Vienna Follow-Up Meeting*, which states that *"[j]ournalists ... are free to seek access to and maintain contacts with, public and private sources of information and that their need for professional confidentiality is respected.*"

105 *Op. cit.* footnote 5, par 20 (2010 UN SRCT Compilation).

106 ibid. Practice 13 (2010 UN SRCT Compilation).

107 The lack of external review was decisive in a judgment of the ECtHR holding that Bulgarian legislation on secret surveillance was incompatible with Article 8: ECtHR, *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria* (Application no. 62540/00, judgment 28 June 2007), par 85.

108 See e.g., ECtHR, *Klass and Others v. Germany* (Application no. 5029/71, judgment of 1978), pars 55-56.

109 ibid par 100: "[i]t is obvious that when surveillance is ordered and while it is under way, no notification of the persons concerned is possible, as such notification would jeopardise the surveillance's effectiveness. They are therefore of necessity deprived of the possibility to challenge specific measures ordered or implemented against them. However, this does not mean that it is altogether impossible to provide a limited remedy – for instance, one where the proceedings are secret and where no reasons are given, and the persons concerned are not apprised whether they have in fact been monitored – even at this stage". Examples of such remedies may include the possibility for individuals believing themselves to be under surveillance to, albeit in exceptional cases, complain to the commission overseeing the system of secret surveillance and also apply to the German Federal Constitutional Court (see ECtHR, *Klass and Others v. Germany* (1978), par 78); see also *Weber and Saravia v. Germany*, par 57); to initiate recourse before a special tribunal (see EComHR, *Christie v. United Kingdom* (Application no. 21482/93, decision of 27 June 1994), pars 122-23, 128-29 and 136-37); to appeal to the Council of State (see EComHR, *Mersch and Others* (decision of 10 May 1985), par 118); to bring complaints were possible to a control committee (see EComHR, *L. v. Norway*, Application no. 13564/88, decision of 8 June 1990, pars 216 and 220).

63. Although there is a preference for judicial remedies,[110] it is widely recognised that the capacity of ordinary courts to serve as an adequate remedy against infringements of human rights in the security field is limited, for example by public immunity, national views on justiciability and standing requirements. Many countries have therefore developed alternative procedures for individuals who claim to have been adversely affected by the security and intelligence services to have avenues of redress before an independent body. These fall generally into three categories: independent officials or ombudspersons (as in the Netherlands), parliamentary bodies (for example, Norway and Romania), or specialist tribunals (as in the United Kingdom).[111] In any case, **adequate mechanisms for supervising the implementation of secret surveillance measures should be provided, which is independent from the authorization process, while ensuring that the persons subjected to such special investigative measures shall be notified in due course** (when this no longer jeopardize confidential methods) and generally that **effective remedies are accessible, in law and in practice**.[112] **The Draft SSU Law should be supplemented in that respect**.

64. Finally, one piece of legislation which is also of relevance is the *Law of Ukraine "On Counterintelligence Activity"*, which regulates surveillance activities carried out by the SSU. While a full legal analysis of this Law is beyond the scope of this Opinion, it appears from a cursory review that some of its provisions may not fully comply with the above-mentioned international standards and recommendations (see par 59 *supra*), especially as regards the unclear personal, material and temporal scope of such surveillance activities and lack of substantive and procedural safeguards and oversight.[113] Since the Draft SSU Law foresees that all surveillance activities will be consolidated under the SSU, **it is essential that the Draft SSU Law or any other relevant legislation clearly and strictly specifies the personal, material and temporal scope of SSU's targeted surveillance powers as well as substantive and procedural safeguards for conducting covert surveillance, which should include as a minimum, the elements and criteria established by the ECtHR and referred to in Practice 21 of the *UN SRCT Compilation***.

5.2.2. Mass Surveillance

65. It is not clear from the Draft Amendments whether the SSU will also be empowered to carry out not only targeted surveillance (which is triggered by a concrete prior suspicion and subject to prior judicial authorization), but also potentially strategic (untargeted) surveillance (which sifts through large quantities of data to detect possible dangers to national security). This distinction is relevant to determine the rules and conditions that govern intelligence-gathering. As opposed to targeted surveillance, mass surveillance programmes do not allow for an individualized case-by-case assessment of the

[110] See further comments on judicial oversight, below.

[111] Further discussion of the respective merits of these approaches can be found can be found in *op. cit.* footnote 5, (2007 Venice Commission's *Report on the Democratic Oversight of the Security Services)*.

[112] See e.g., ECtHR, *Zakharov v. Russia* [GC] (Application no. 47143/06, judgment of 3 December 2015), par 238. The absence of a remedy may mean that there is a violation of the ECHR: *Segerstedt-Wiberg v. Sweden* (Application no. 62332/00, judgment of 6 June 2006). The ECtHR has stressed that, even in the context of national security, the remedy required by Article 13 must be effective *in practice* as well as in law; see ECtHR, *Al-Nashif v. Bulgaria* (Application no. 50963/99, judgment of 20 June 2002), par 136.

[113] For instance, the list of permissible objectives of intelligence collection appears overly vague; the Law does not clearly and restrictively defines categories of persons and activities which may be subject to surveillance; the threshold of suspicion is not explicitly stipulated in the Law; the duration for implementing surveillance activities is not strictly limited (in that respect, the ECtHR criticized domestic legislation because it did not lay down a clear limitation in time for the authorization of a surveillance measure; see ECtHR, *Iordachi and Others v. Moldova* (Application no. 25198/02), par 45)); the procedures for authorizing, overseeing and reviewing the use of surveillance activities are not sufficiently stipulated in the Law; there is a lack of substantive and procedural safeguards, especially the lack of ex-ante judicial authorization since the surveillance activities simply require authorization by SSU management (the only clear ex-ante involvement of the judiciary is foreseen when the SSU uses surveillance methods in the context of "operational investigations" which are conducted in the frame of criminal investigations but the judicial authorization is not explicitly mentioned elsewhere in the Law, relating to any other surveillance function of the SSU); and Article 12 of the Law refers to oversight of the surveillance in a very general and vague manner, without specifying which actors are mandated to scrutinize which aspects of surveillance, among others.

proportionality prior to such measures being employed and therefore appear to undermine the very essence of the right to respect for private and family life.[114]

66. The ECtHR has considered that the decision to operate a bulk interception regime in order to identify unknown threats to national security falls within States' margin of appreciation.[115] Similarly, the Venice Commission has recognized the intrinsic value of strategic surveillance for security operations, since it enables the security services to adopt a proactive approach, looking for hitherto unknown dangers.[116] However, both the ECtHR and the Venice Commission have stressed that such a prerogative constitutes a high risk for violations of human rights, particularly the right to respect for private and family life and should be subject to very strict limitations and safeguards. This is important in light of the caselaw of the ECtHR, which has found surveillance systems that allow for the interception of communications and masses of data of virtually anyone in a country to be violating the right to privacy, especially where the ordering of such measures is taking place entirely within the realm of the executive and without an assessment of strict necessity.[117]

67. The Court has held that the above-mentioned six minimum requirements related to targeted surveillance (see par 58 *supra*) should also apply to strategic surveillance.[118] The ECtHR has also expressed concerns in the absence of robust independent oversight of the entire selection process, including the selection of bearers for interception, selectors and search criteria for filtering intercepted communications, and the selection of material for examination by an analyst.[119] The absence of any real safeguards applicable to the selection of related communications data for examination has also been held to be problematic.[120]

68. In light of the foregoing, if the SSU is indeed allowed to undertake strategic surveillance, **the Draft SSU Law should clearly and strictly circumscribe the SSU's powers to conduct such surveillance**, and the said provisions should comply with the principles of **legality, necessity and proportionality. The above-mentioned minimum safeguards developed by the ECtHR for other types of surveillance shall be reflected** (types of surveillance, permissible objectives, duration and renewal of such measures, as well as robust independent oversight of the entire selection process, including the selection of bearers for interception, the selectors and search criteria for filtering intercepted communications, and the selection of material for examination by an analyst).[121] Moreover, the ECtHR has considered that judicial authorization constitutes a "*best practice*" and an additional important safeguard, though by itself it can neither be necessary nor sufficient to ensure compliance with Article 8 of the ECHR.[122] **The drafters should consider introducing judicial authorization as an additional safeguard.**

---

114 See UN Special Rapporteur on counter-terrorism, *2014 Annual Report to the UN General Assembly*, 23 September 2014, A/69/397: par 52; and *Report to the UN Human Rights Council*, 21 February 2017, A/HRC/34/61, pars 10-13. For discussion of legislation in EU countries on strategic/mass surveillance, see EU Fundamental Rights Agency, *Mapping of legal frameworks on Surveillance by Intelligence Services within the EU* (2015).

115 See e.g., ECtHR, *Big Brother Watch and Others v. the United Kingdom* (Application nos. 58170/13, 62322/14, 24960/15, judgment of 13 September 2018, referred to the Grand Chamber on 4 February 2019), par 314.

116 See e.g., *op. cit.* footnote 5, par 101 (2015 Venice Commission *Report on the Democratic Oversight of Signals Intelligence Agencies).*

117 See e.g., ECtHR, *Szabo and Vissy v. Hungary* (Application no. 37138/14, judgment of 12 January 2016); and *Roman Zakharov v. Russia* [GC] (Application no. 47143/06, judgment of 5 December 2015).

118 See ECtHR, *Big Brother Watch and Others v. the United Kingdom* (Application nos. 58170/13, 62322/14, 24960/15, judgment of 13 September 2018, referred to the Grand Chamber on 4 February 2019), par 315.

119 ibid. pars 347 and 387 (2018 ECtHR, *Big Brother Watch and Others v. the United Kingdom*, referred to the Grand Chamber).

120 ibid. par 387.

121 *Op. cit.* footnote 5, Practices 20-23 (2010 UN SRCT Compilation).

122 *Op. cit.* footnote 118, par 320.

5.2.3. Interception of telecommunications

69. The interception of telecommunications is referred to by the Draft SSU Law in several provisions (Article 12.1 (20) and (22) and Article 13.8). The latter explicitly tasks the SSU with this power, but it does not stipulate the procedures for telecommunication interceptions. It simply states that SSU obtains from telecommunication companies all sorts of information, including information on the users, as well as both the metadata and content of the communication, as per the procedure established by law. **It is recommended to specify which laws are applicable**.

70. **Detailed procedures on how telecommunication interception should be requested, reviewed, authorised, implemented and overseen reflecting the above-mentioned minimum safeguards shall be included in such legislation or in Article 13.8 of the Draft SSU Law**. Actually, legislation governing telephone tapping in several countries has failed the quality of law test where it did not indicate with reasonable clarity the extent of discretion conferred on the authorities concerning these matters, e.g. concerning whose telephone could be tapped, for what alleged offences, for how long, and concerning the destruction of recordings and transcripts.[123]

71. Moreover, it is a good practice for the authorization of the most intrusive intelligence collection methods (e.g. the interception of the content of communications, the interception of mail and surreptitious entry into property) to include senior managers in intelligence services, the politically accountable executive and a (quasi) judicial body.[124] Indeed, the ECtHR ruled on many occasions regarding the necessity of an external assessment of whether interception of communications was strictly necessary and whether there are effective remedial measures in place. It also held that when the ordering of the interception of telecommunications is taking place entirely in the realm of the executive, this amounted to a violation of Article 8 of the ECHR.[125] **Article 13.8 of the Draft SSU Law or other legislation as appropriate should include such a safeguard.**

5.2.4. Processing, Storing and Destruction of Personal Data

72. Article 13.4 states that "*[i]ntelligence data necessary for achieving the objectives and performing the tasks set to the [SSU] shall be obtained in accordance with the procedure established by law and acts of the President of Ukraine"*. Article 14.5 of the Draft SSU Law further states that "*information…. shall be processed and stored in accordance with the procedure and within the time limits specified by law*". **It is recommended to specify which legislation is applicable.**

73. The *UN SRCT Compilation* stresses the need that *"[p]ublicly available law outlines the types of personal data that intelligence services may hold, and which criteria apply to the use, retention, deletion and disclosure of these data"* and that *"[i]ntelligence services are permitted to retain personal data that are strictly necessary for the purposes of fulfilling their mandate"*.[126] The information collected by security agencies shall be used to the minimum extent necessary and only for the reasons justifying interference with privacy in the first place. In the case of *Liberty and Others v. the United Kingdom*,[127] concerning interception of telecommunications, the ECtHR found that the procedure to be followed for selecting for examination, sharing, storing and destroying intercepted

[123] See e.g., ECtHR, *Kruslin v. France* (Application no. 11801/85, judgment of 24 April 1990); *Huvig v. France* (Application no. 11105/84, judgment of 24 April 1990); *Valenzuela Contreras v. Spain* (Application no. 27671/95, judgment of 30 July 1998); *Amann v. Switzerland* [GC] (Application no. 27798/95, judgment of 16 February 2000).
[124] *Op. cit.* footnote 5, par 35 (2010 UN SRCT Compilation).
[125] See e.g., ECtHR, *Szabo and Vissy v. Hungary* (Application no. 37138/14, judgment of 12 January 2016), pars 74-75 and 89.
[126] *Op. cit.* footnote 5, Practice 23 (2010 UN SRCT Compilation).
[127] ECtHR, *Liberty and Others v. the United Kingdom* (Application no. 58243/00, judgment of 1 July 2008), par 69. 9

material had not been accessible to the public and therefore found a violation of Article 8 of the ECHR.

74. **It is therefore essential that the Draft SSU Law, or relevant legislation to which the Draft SSU Law should make a cross-reference, clearly stipulates the procedures for examining, using, and storing the data intercepted by the SSU, the precautions to be taken when communicating the data to other parties, the duration (not excessively long) of such measures[128] and the circumstance in which recordings may or must be erased or destroyed.[129] Or a cross-reference could be made to relevant legislation, providing that it is compliant with international human rights standards and include such safeguards**. It is also good practice that a security service proactively informs the general public about the type of personal data it keeps as well as permissible grounds for the retention of personal information by an intelligence service.[130] It is also important to stipulate that intelligence services are not allowed to store personal data on discriminatory grounds and criminalizing the disclosure or use of personal data by intelligence officers outside the established legal framework.[131] It is also essential to provide for an obligation on the intercepting agencies to keep records of interceptions to ensure that the supervisory body has effective access to details of surveillance activities undertaken.[132] **The legal drafters could consider including such aspects in the Draft SSU Law.**

75. It is worth emphasizing that, as per the ECtHR judgement on *Weber and Saravia v. Germany*, **it is important to provide guidelines for the management and use of personal data by intelligence services**.[133] Some guidance and practices on the collection and use of personal data by security services are outlined in the *UN SRCT Compilation* (Practices 21-25) and can serve as a useful reference.

5.2.5. Telecommunication Operators' Obligation to Install Equipment Necessary for Implementing Detective and Counterintelligence Measures

76. The proposed amended Article 39.4 of the Law "On Telecommunications" provides an obligation for the telecommunication operators to install equipment necessary for implementing detective and counterintelligence measures, at their own costs. It is not clear whether this means giving the SSU and law enforcement authorities direct access to all mobile-telephone communications of all users, without requiring them to obtain prior judicial authorization.

77. It is worth noting that in the case of *Zakharov v. Russia*, a similar scheme was provided which gave the security services technical means to circumvent the authorization procedure and to intercept any communications without obtaining prior judicial authorization. The ECtHR concluded that such a mechanism violated Article 8 of the ECHR since the supervision of interceptions did not comply with the requirements of

---

[128] See e.g., ECtHR, *Segerstedt-Wiberg v. Sweden* (Application no. 62332/00, judgment of 6 June 2006), where the Court found that the Swedish government had violated Article 8 of the ECHR when it retained personal data in a security file for a period exceeding thirty years; in view of the nature and age of the information, the court did not accept the defence that the decision to continue storing the information was supported by relevant and sufficient reasons of national security.

[129] See, for example, the detailed analysis of the German G10 law in ECtHR, *Weber and Saravia v. Germany* (Application no. 54934/00, decision of 29 June 2006); and *Roman Zakharov v. Russia* [GC] (Application no. 47143/06, judgment of 5 December 2015), par 231. See also e.g., ECtHR, *Rotaru v. Romania* (Application no. 28341/95, judgment of 4 May 2000), par 57 where the Court found that the Romanian law on the regulation of security files breached Art 8 because it was insufficiently clear in describing the uses to which the personal information in the files could be put and did not establish any mechanism for monitoring the use of the information (in particular, the law did not define the kind of information that could be recorded, the categories of people against whom surveillance measures could be taken, the circumstances in which such measures could be taken, and the procedures to be followed. Nor did it include any limitations on the length of time for which it could be held).

[130] For instance, the Section 11 of the *Canadian Security Intelligence Act* prescribes the procedures for processing, retention, destruction of datasets.

[131] *Op. cit.* footnote 5, par 37 (2010 UN SRCT Compilation).

[132] See e.g., ECtHR, *Roman Zakharov v. Russia* [GC] (Application no. 47143/06, judgment of 5 December 2015), par 272.

[133] ECtHR, *Weber and Saravia v. Germany* (Application no. 54934/00, judgment of 29 June 2006), pars 93-95.

independence, powers and competence to exercise an effective and continuous control, public scrutiny and effectiveness in practice, while also noting the lack of access to effective remedies.

78. Additionally, the UN Human Rights Committee has considered that any restriction on the operation of information dissemination systems, including that of internet service providers, is not legitimate unless it conforms with the test for restrictions on freedom of expression under international law.[134] It is unclear what would be the cost of installing and maintaining such equipment and whether the said provision also implies an obligation for the systematic retention by service providers of data. If this is the case, it is worth mentioning that at the EU level, the Court of Justice of the European Union concluded that the compulsory systematic retention of data by internet service providers, without being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary, constituted a disproportionate interference with fundamental rights and freedoms.[135]

79. In light of the foregoing, given the potential to circumvent the requirement of prior judicial authorization and the burden imposed on telecommunications operators, **the drafters should reconsider such an obligation and in any case, judicial authorization should be required by the SSU for accessing the intercepted communications**.

5.2.6. Access to one's own data held by the SSU

80. The Draft SSU Law does not include provisions regarding the data protection of data subjects, i.e. persons whose data is collected and processed by the SSU. In this respect, the *Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* - which entered into force in Ukraine on 1 January 2011 - explicitly recognizes the rights of data subjects. Article 8 of the CoE Convention provides for clear obligations for public authorities to respond to requests concerning the existence of personal data, to communicate the data to the data subject, to rectify or erase in case of an unlawful collection/processing,[136] though there are exceptions in the interests of "*protecting State security*". These standards are not only recognized by the CoE Convention, but also the international soft-law instruments such as the 1988 *UN Guidelines for the Regulation of Computerized Personal Data Files* (Principle 4), *The Tshwane Principles* (Part III), as well as the *UN SRCT Compilation* (Practice 26).

81. In line with such international standards and recommendations, most democratic countries have adopted laws and established mechanisms to protect and fulfill the right to access one's own data.[137] **Article 15 of the Draft SSU Law should be revised to include provisions regulating access to one's own data, in view of international standards and good practices outlined above. There should also be complaints or**

---

134 See UN Human Rights Committee, *General Comment No. 34 on Freedom of Opinion and Expression*, 12 September 2011, par 43.

135 See Court of Justice of the European Union, *Digital Rights Ireland Ltd v. Ireland*, 8 April 2014, C-293/12, pars 58 to 69.

136 Article 8 of the Convention states that: "*Any person shall be enabled: a) to **establish the existence of an automated personal data file**, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file; b) to **obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored** in the automated data file as well as **communication to him of such data** in an intelligible form; c) to obtain, as the case may be, **rectification or erasure of such data if these have been processed contrary to the provisions of domestic law** giving effect to the basic principles set out in Articles 5 and 6 of this Convention; d) to **have a remedy** if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with*".

137 There are different approaches regarding the access to the personal data of the data subject. In 12 EU Member States including Austria, Belgium, Bulgaria, Cyprus, Finland, France, Hungary, Ireland, Italy, Luxembourg, Portugal and Sweden; Data Protection Authorities and /or expert oversight bodies are mandated to access the data on behalf of the data subject to check whether the justification for restricting the data subject's access was reasonable, access and review the said data to see if it was collected lawfully, and order the destruction of the data if there was any violation of laws. See also Germany, which adopted a novel approach whereby the security services have a general obligation to inform the targets of surveillance, after the surveillance measure has ended (Germany G-10 Law, Section 12. There are however caveats and conditionality's applicable). See also EU FRA, *Surveillance by Intelligence Services*, Vol 2, (2017), pages 110 and 126.

compensation procedures for affected individuals whose personal data is collected, stored and used unlawfully.[138]

5.2.7. Use of Undercover Agents or Contractors

82. Article 12.1 (25) and (26) focuses on undercover agents or contractors. Article 12.1 (25) provides the SSU with the power to contract natural and legal persons as undercover agents. However, this provision also allows for the "*voluntary assistance of persons for covert cooperation on a confidential basis*". In such a context, it may be difficult to determine if a person is voluntarily assisting the SSU, or coerced to conduct undercover acts. Moreover, undercover actions as part of covert information collection can be highly intrusive and therefore should be based on proper documentation, so that it is traceable by oversight authorities. As per Council of Europe guidance, undercover operations should be properly authorized, recorded, supervised and scrutinized.[139] Indeed, the inherently secret nature of undercover work, combined with the lack of ex-ante control on the application of undercover policing methods leaves very little room for effective judicial oversight, or any other external oversight for that matter. In most cases, undercover methods of the law enforcement come into scrutiny *ex-post facto*, following complaints and lawsuits filed against law enforcement officers. **Article 12.1 (25) of the Draft SSU Law should be revised to remove the reference to "voluntary" undercover actors, while ensuring that there is some form of documentation formally evidencing the delegation/tasking of undercover acts by the SSU to a natural or legal person, and detailed authorization, supervision and oversight procedures**.

83. While acknowledging the necessity, in certain circumstances, to resort to certain under-cover/covert inquiries or investigations to identify and investigate offences, the ECtHR has also considered that the use of such proactive policing methods should be subject to certain limitations. Especially when this involves actively testing an individual's integrity, the state must ensure that this method does not instigate the commission of a crime, more specifically, that the state officials did not persuade and talk the person into committing such crime and that the person was already ready and willing to commit the crime before his/her interaction with State agents.[140] Moreover, the collection of information or recording by a state official of an individual without his or her consent would raise issues with respect to the right to respect for private life protected under Article 8 of the ECHR.[141] **Such limitations should be reflected in provisions concerning the use of covert agents or contractors**.

5.3. Information Collection and Processing

84. Article 13 of the Draft SSU Law authorizes the SSU to collect information (including personal data) from open sources (Article 13.2), from other law enforcement, public and military bodies (Article 13.3), by interception of communications and other covert means (Article 13.5), through direct access to official databases (Article 13.6) and on request or by court order to equivalent private systems, together with CCTV and similar systems (Article 13.7), and to "communications data" (Article 13.8). Subsequent provisions govern the use of information obtained or created by the SSU (Article 14) and its processing and supply to other official bodies (Article 15).

---

[138] For discussion of complaints mechanisms in EU countries on strategic surveillance; see *op. cit.* footnote 114 (2015 EU FRA's *Mapping of legal frameworks on Surveillance by Intelligence Services within the EU*).

[139] See Council of Europe, *The Deployment of Special Investigative Means* (2013), pages 48-52.

[140] See e.g., ECtHR, *Ramanauskas v. Lithuania*, ECtHR [GC] (Application no. 74420/01, judgment of 5 February 2008), par 73.

[141] See e.g., ECtHR, *Klass and Others v. Germany* (Application no. 5029/71, judgment of 1978), pars 36-38; and *Vetter v. France*, (Application no. 59842/00, judgment of 31 August 2005), par 27.

85. Compared to recent legislation in other European countries on the equivalent topics, these provisions are extremely sparse and lacking details and safeguards, to the extent of potentially leading to violations of the rights to respect for private and family life and to an effective remedy (see also par 12 *supra* on profiling and collection and automatic processing of sensitive data).

5.3.1. Monitoring of Open Sources

86. Article 13.2 of the Draft SSU Law provides that the SSU "*shall monitor open sources of information and take other measures aimed at gathering information necessary to fulfil the tasks set to the [SSU]*". The ECtHR has considered that the systematic collection and storing of data by security services on particular individuals constituted an interference with these persons' private lives, even if such data were collected in a public place.[142] Moreover, according to the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, "*States and intergovernmental organizations should refrain from establishing laws or arrangements that would require the 'proactive' monitoring or filtering of content, which is both inconsistent with the right to privacy and likely to amount to prepublication censorship*".[143] Such interference must be supported by relevant and sufficient reasons and must be proportionate to the legitimate aim(s) pursued.[144]

5.3.2. Direct Access to Databases without a Warrant

87. Article 13.6 provides the SSU with "direct free-of-charge access to automated information and reference systems, records, registries, databanks or databases maintained or administered by public authorities, local self-government bodies, state-owned enterprises, institutions, organisations". There are a few issues with giving such a blanket power to the SSU. First, this is an unchecked power, whereby no independent or judicial authority is mandated to carry out the ex-ante review of the legality, necessity and proportionality of the direct and unlimited access to such databases compared to the objectives of the surveillance. The lack of any supervision clearly derogates from the aforementioned standards as set out by the ECtHR. Second, the scope of the access is so broad, that it does not only cover the databases of public authorities, but it also allows to access state-owned enterprises' and other "organizations" databases. There may be enterprises which are partially state-owned, and this article would still allow for direct access. By way of example, access to a partially state-owned telecommunication company would allow for warrantless interception of metadata and content of millions of customers, without any oversight. **Consequently, access to databases, databanks, registrars of enterprises or organizations, whether they are state-owned or not, should be subject to independent and effective authorization and supervision, preferably by a judicial authority**.

5.3.3. Direct Access to Audio/video Information Systems and Physical Storages

88. Article 13.7 of the Draft SSU Law extends the scope of SSU's direct access even further to fixed and mobile radio-monitoring systems and devices, audio, video and audio/video surveillance, automated information and reference systems, records, registries, databanks or databases, documents, other physical storage media owned by the data holders referred

[142] See e.g., ECtHR, *Peck v. the United Kingdom* (Application no. 44647/98, judgment of 28 January 2003), par 59; and *P.G. and J.H. v. the United Kingdom* (Application no. 44787/98, judgment of 25 September 2001), pats 57-59.

[143] See UN Special Rapporteur on freedom of opinion and expression, Report on the Regulation of User-generated Online Content, A/HRC/38/35, 6 April 2018, par 67

[144] See e.g., ECtHR, *Segerstedt-Wiberg v. Sweden* (Application no. 62332/00, judgment of 6 June 2006), par 88.

to in Article 13.6. The latter provision allows for SSU's access to "*analogous physical information storage media belonging to individuals and/or non-state enterprises, institutions, organisations – with their consent or under the court order*". This essentially empowers the SSU to seize personal belongings such as phones, cameras, laptops, storage devices and process the information in them. It is important to note that ex-ante judicial authorisation for such a far-reaching power is introduced as a safeguard for the latter power. However, the law refers to seizing such items either "with the consent" or "under the court order". As explained earlier in this section, **consent of the person subject to intrusive methods does not constitute an effective safeguard and should be removed from Article 13.6, while ensuring that the SSU's use of intrusive methods is systematically subject to judicial authorization**.

5.4. Information-sharing with Domestic Agencies

89. Various articles of the Draft SSU Law touch upon information-sharing between the SSU and other agencies in Ukraine. Article 13.3 stipulates the unrestricted power of the SSU to receive any information from "*law enforcement and other public authorities, military units, local self-government bodies, enterprises, institutions, organisations, regardless of their form of ownership, and individuals within three working days, upon a request signed by the SSU management*". The *UN SRCT Compilation* provides that *"[i]ntelligence-sharing between intelligence agencies of the same State or with the authorities of a foreign State is based on national law that outlines clear parameters for intelligence exchange, including the conditions that must be met for information to be shared, the entities with which intelligence may be shared, and the safeguards that apply to exchanges of intelligence*".[145]

90. Even though Article 13.3 states that the information will be received "*according to the established procedure*", the Draft SSU Law does not elaborate on those procedures. Moreover, this provision does not limit the scope of information that the SSU is entitled to receive. The SSU should not be entitled to receive just "any information" but instead it should receive information that falls strictly under its competence. Further, the decision on information-sharing is entirely within the discretion of the senior management of the SSU. As mentioned before, since some of the information shared may be personal data and fall under Article 8 of the ECHR, its sharing should be subjected to scrutiny and to effective remedy, where violations occur. **Article 13.3 of the Draft SSU Law should be more strictly circumscribed and amended according to these principles**.

91. Articles 14.1 and 14.2 regulate sharing of information by the SSU with other public authorities. Article 14.1 narrowly lists the "consumers of intelligence" as the "*President of Ukraine, Chairperson of the Verkhovna Rada of Ukraine, Prime Minister of Ukraine, Secretary of the National Security and Defence Council of Ukraine, as well as public agencies that are part of the security and defence sector of Ukraine*". However, Article 14.2 (2) makes it possible for the SSU to share information with a wide range of stakeholders including "*another public authority, enterprise, institution, organisation in compliance with the requirements for protection of restricted access information stipulated by law*".

92. Article 14.3 of the Draft SSU Law provides a legal safeguard against misuse of intelligence, by stating that information obtained as part of SSU's surveillance activities cannot be used in criminal proceedings,[146] which is welcome in principle. However,

---

[145] *Op. cit.* footnote 5, Practice 31 (2010 UN SRCT Compilation).

[146] The section on Final and Transitional Provisions of the Draft Law, in amending the *Law of Ukraine "On Organisational and Legal Foundations of Combating Organised Crime",* Article 16.4, states that *'[t]he terms of and procedure for information sharing between*

Article 14.3 also introduces an exception to that safeguard by exempting criminal proceedings stipulated in the Law on Counterintelligence Activities. Article 7.6 of the Law on Counterintelligence Activities allows the SSU to use counterintelligence capabilities in the context of criminal investigations relating to terrorism and other attacks on the state security of Ukraine. This function of the SSU is exceptionally put under the supervision of the investigating judge and the prosecutor (who approves the use of SSU surveillance for criminal investigations), and the Attorney General, who is tasked with supervising the observance of laws. While Article 14.3 constitutes an important safeguard, it does not **elaborate on the measures to prevent such information-sharing with criminal justice institutions, and what happens when that rule is breached (in terms of criminal and disciplinary liability for officers doing so) and should be supplemented in that respect**.

93. In light of the foregoing, **Articles 13.3, 14.1 and 14.2 of the Draft SSU Law should be revised by elaborating on the procedures and safeguards applicable to information sharing between the SSU and other domestic agencies. Such detailed regulation should enable the oversight authorities to scrutinize the terms, purposes and necessity of information sharing *ex-post facto***.

5.5. Information Exchange and Co-operation with Foreign Security Services

94. Article 19 of the Draft SSU Law regulates the "*[c]o-operation and interaction of the [SSU] with authorities and institutions of foreign states and international organisations*", while Article 20 specifies the rules concerning information sharing in the context of international co-operation, including requiring President's approval, a written record and compliance with Ukrainian legislation, which is welcome and overall in line with Practice 32 of the *UN SRCT Compilation*. These requirements are essential safeguards to create a paper track, which could be examined by judicial authorities if need arise. There are however no other specific limitations stated in such provisions regarding international co-operation. The *UN SRCT Compilation* provides a number of good practices to enhance foreign intelligence sharing's compliance with international law and human rights standards.[147] The ECtHR case law also points out to the importance of external supervision and remedial measures.[148] Generally, co-operation between security services may risk circumventing the existing national mechanisms of control.[149] To prevent such risks, it is important that the Draft SSU Law clearly provides additional substantive and procedural safeguards, especially in terms of handling and sharing of personal data, and other human rights considerations.

---

the authorised operational units of the Security Service of Ukraine and the units of the National Police bodies shall be regulated by joint acts of the Ministry of Internal Affairs of Ukraine and the Security Service of Ukraine" provides also a safeguard; since it aims to regulate information sharing between SSU and domestic law enforcement. However the content of the joint acts should be subject to external oversight.

147 *Op. cit.* footnote 5, Practice 31 (2010 UN SRCT Compilation). **Practice 32,** *states that "National law outlines the process for authorizing both the agreements upon which intelligence-sharing is based and the ad hoc sharing of intelligence. Executive approval is needed for any intelligence-sharing agreements with foreign entities, as well as for the sharing of intelligence that may have significant implications for human rights";* **Practice 33**. *"Before entering into an intelligence-sharing agreement or sharing intelligence on an ad hoc basis, intelligence services undertake an assessment of the counterpart's record on human rights and data protection, as well as the legal safeguards and institutional controls that govern the counterpart. Before handing over information, intelligence services make sure that any shared intelligence is relevant to the recipient's mandate, will be used in accordance with the conditions attached and will not be used for purposes that violate human rights";* and **Practice 35** *"Intelligence services are explicitly prohibited from employing the assistance of foreign intelligence services in any way that results in the circumvention of national legal standards and institutional controls on their own activities. If States request foreign intelligence services to undertake activities on their behalf, they require these services to comply with the same legal standards that would apply if the activities were undertaken by their own intelligence services".*

148 In *Szabo and Vissy v. Hungary,* the ECtHR stated that *"[t]he governments' more and more widespread practice of transferring and sharing among themselves intelligence retrieved by virtue of secret surveillance – a practice, whose usefulness in combating international terrorism is, once again, not open to question and which concerns both exchanges between Member States of the Council of Europe and with other jurisdictions – is yet another factor in requiring particular attention when it comes to external supervision and remedial measures";* ECtHR, *Szabo and Vissy v. Hungary* (Application no. 37138/14, judgment of 12 January 2016), par 78.

149 See e.g., *op. cit.* footnote 5, par 74 (2015 Venice Commission's *Report on the Democratic oversight of Signals Intelligence Agencies*).

95. In light of the foregoing, **it is recommended to supplement Articles 19 and 20 of the Draft SSU Law to provide that before entering into an information and intelligence sharing agreement, or doing so on an *ad hoc* basis, an assessment should be made of the counterpart's record on human rights and data protection, as well as of the legal safeguards and institutional controls that govern the counterpart.**[150] **There should also be a clear undertaking not to transfer intelligence which is likely to be used for purposes that violate human rights,** e.g., that would ultimately result in torture or other ill-treatment or would enable a country to repress free speech or human rights defenders or allow further human rights violations.[151] **Articles 19 and 20 of the Draft SSU Law should also make a reference to necessary conditions and procedures before any information is shared with a foreign intelligence service** (assessment of the necessity for sharing the information, relevance of the information to the counterpart's mandate, human rights considerations). Furthermore, **it would be advisable to add a specific provision explicitly prohibiting the SSU to seek the support of foreign counterparts' surveillance capacities to circumvent the requirements and standards applicable under Ukraine's national legal framework**.[152] Finally, **the Draft SSU should expressly mandate oversight bodies to scrutinize international intelligence cooperation**, including the compliance with the Ukrainian legislation and international human rights standards of agreements and security service co-operation with foreign bodies, the exchange of information, joint operations and the provision of equipment and training.[153]

5.6. Use of Coercive Measures, including Firearms

96. Pursuant to Article 16 of the Draft SSU Law, SSU personnel may use "*coercive measures on the grounds*", in accordance with the procedure established by the *Law of Ukraine "On the National Police"*, which means that this may include the use of physical force, special tools and firearms as detailed in Articles 42-46 of that Law. **This should be reconsidered or its usage kept to an absolute minimum, in light of the high risks of human rights violations.** Article 16 gives SSU staff the powers to use weapons and other physical coercion and special means, without any special restriction on SSU staff using lethal force.

97. ODIHR has previously reviewed a draft of the *Law of Ukraine on Police and Police Activities*, where it provided recommendations in terms of the use of coercive measures, including firearms.[154] While the analysis of the *Law of Ukraine "On the National Police"* goes beyond the scope of this Opinion, the use of such coercive measures should strictly comply with international standards and recommendations, including the right to life (Article 6 of the ICCPR, Article 2 of the ECHR), the *UN Code of Conduct for Law Enforcement Officials* (1979) and the *UN Basic Principles on the Use of Force and Firearms by Law Enforcement Officials* (1990). The right to life requires the State not only to refrain from the intentional and unlawful taking of life, but also to take appropriate steps to safeguard the lives of those within its jurisdiction. This applies for example to the planning and supervision of SSU operations involving firearms.

---

[150] ibid. Practice 33 (2010 UN SRCT Compilation). See also ODIHR, *Guidelines on Addressing the Threats and Challenges of "Foreign Terrorist Fighters"* (2018), page 43.

[151] *Op. cit.* footnote 5, par 75 (2015 Venice Commission's *Report on the Democratic oversight of Signals Intelligence Agencies*). See also ibid. Practice 33 (2010 UN SRCT Compilation); and ODIHR, *Guidelines on Addressing the Threats and Challenges of "Foreign Terrorist Fighters"* (2018), page 43.

[152] *Op. cit.* footnote 5, Practice 35 (2010 UN SRCT Compilation).

[153] *Op. cit.* footnote 5, Recommendation 5 (2015 CoE Commissioner for Human Rights *Democratic and Effective Oversight of National Security Services*).

[154] See *ODIHR Opinion on the Draft Law of Ukraine on Police and Police Activities* (1 December 2014).

98. From a cursory review of Article 46 of the *Law of Ukraine "On the National Police"* relating to the use of firearms, it appears that the grounds for their usage go beyond those envisaged at the international level.[155] Moreover, the Law does not seem to provide for all the limitations and safeguards contemplated at the international level, especially concerning the use of lethal force. **ODIHR stands ready to review the Law of Ukraine "On the National Police" to assess its compliance with international human rights standards and OSCE commitments**. In the meantime, **it may be advisable to provide in the Draft SSU Law limitations and safeguards in line with international standards, especially regarding the use of firearms and of lethal force**.

99. It is also crucial that relevant SSU personnel be duly trained on the use of coercive measures, especially a special training on the use of firearms, including on issues of police ethics and human rights, to alternatives to the use of force and firearms, and to technical means, with a view to limiting the use of force and firearms.[156] **This should be provided in the Draft SSU Law**. **It is also essential to clearly state the prohibition for the SSU to resort to torture or other cruel, inhuman or degrading treatment or punishment, including sexual and gender-based violence, in all circumstances. Accessible and effective independent complaints mechanisms should also be in place in case of unlawful use of force and firearms or torture or other cruel, inhuman or degrading treatment or punishment. The Draft SSU Law should be supplemented in that respect**.

5.7. Arrest and Detention

100. It is not clear in the Draft SSU Law whether SSU personnel have the power of arrest and detention, though Article 12.1 (41) provides that they may "*pursue and detain persons suspected of committing [criminal offences]*". However, such provision does not specify under which circumstances and in which facilities such detention should be allowed, nor does the Draft Law make reference to other relevant legislation. The *UN SRCT Compilation* says that intelligence services should not be given "*powers of arrest and detention if this duplicates powers held by law enforcement agencies that are mandated to address the same activities*".[157] Given the SSU's all-encompassing mandate contemplated by the Draft SSU Law (see Sub-Section 3 *supra*), such vague stipulations giving detention powers to the SSU would carry high risk of ill-treatment, *incommunicado* detention, and extraordinary rendition and other serious human rights violations. **The drafters should reconsider granting the SSU powers of arrest and detention**.

101. In any case, if retained at all, SSU's arrest and detention powers shall be subject to the same conditions and degree of oversight as applies to their use by law enforcement authorities, and shall be carried out in strict compliance with Article 9 of the ICCPR, Article 5 of the ECHR, as well as the *UN Standard Minimum Rules for the Treatment of Prisoners* (2015). In particular, there should always be a judicial review of the lawfulness of any deprivation of liberty[158] as well as other safeguards (such as prompt access to a lawyer, the right to be informed of the nature of the charge against them from the very outset of deprivation of liberty and to have the fact of one's detention notified to a third party of choice (relative, friend, consulate), the right to request a medical examination

---

[155] The *UN Basic Principles on the Use of Force and Firearms by Law Enforcement Officials* (1990), state that *"[l]aw enforcement officials shall not use firearms against persons except in self-defence or defence of others against the imminent threat of death or serious injury, to prevent the perpetration of a particularly serious crime involving grave threat to life, to arrest a person presenting such a danger and resisting their authority, or to prevent his or her escape, and only when less extreme means are insufficient to achieve these objectives. In any event, intentional lethal use of firearms may only be made when strictly unavoidable in order to protect life"* (Principle 9).

[156] *UN Basic Principles on the Use of Force and Firearms by Law Enforcement Officials* (1990), Principles 19 and 20.

[157] *Op. cit.* footnote 5, Practice 27 (2010 UN SRCT Compilation).

[158] Article 9 par 4 of the ICCPR and Article 5 par 4 of the ECHR. See also ibid. Practices 28 and 30 (2010 UN SRCT Compilation).

and to be informed about their rights and other relevant procedural safeguards as set out in Articles 9 of the ICCPR and Article 5 of the ECHR). **The drafters should ensure that such safeguards are included in the Draft SSU Law or make a cross-reference to the relevant legislation that embed them**.

102. It is also worth noting that **the SSU should not be permitted to deprive persons of their liberty simply for the purpose of intelligence collection**[159] **and this should be explicitly stated in the Draft SSU Law**. Furthermore, **the SSU should also not be permitted to operate its own detention facilities or to make use of any unacknowledged detention facilities operated by third parties,**[160] **and rather utilize pre-trial detention facilities used under the criminal justice system.** In addition, the **SSU law enforcement powers should be restricted to cases in which there is a reasonable suspicion that an individual has committed or is about to commit a specific criminal offence that poses a national security threat.**[161] **The Draft SSU Law should be supplemented to reflect such limitations, as appropriate**.

5.8. Search, Seizure and Interrogation Powers

103. Article 12.1 (31)-(33) of the Draft SSU Law entrusts the SSU with search, seizure and interrogation powers. Typically, these constitute police powers that are highly intrusive, and may lead to unlawful infringements of privacy as well as potential risks of torture or other ill-treatment. As such, **the implementation of such functions (especially entering private property, search and seizure) should be subjected to ex-ante judicial authorization**.

104. First, it is not clear under which circumstances and conditions the SSU would be allowed to use such broad (police) powers. Second, it is highly concerning that the SSU would be allowed to rely on individuals' "consent" and carry out such tasks without any judicial authorization. Indeed, when faced with armed intelligence/law enforcement officers, individuals are probably unlikely to refuse such consent and to exercise their free will.

105. Accordingly, **these provisions should either be removed altogether from the Draft SSU Law or, if deemed absolutely necessary, the reference to individuals' "consent" should be removed and the implementation of search, seizure and interrogation powers should be exercised only upon ex-ante judicial authorization together with other procedural safeguards applicable under criminal justice systems as set out as appropriate in Articles 9 and 14 of the ICCPR and Articles 5 and 6 of the ECHR** (including access to a lawyer before interrogation, being informed on the nature of the charge against them, being informed about their rights and other relevant procedural safeguards).

5.9. Counterintelligence and Intelligence Activities

106. Article 12.1 (1) of Draft SSU Law gives the SSU the power to provide counterintelligence support to foreign missions, in view of the "*realisation of state interests in the sphere of foreign policy and foreign economic activity*". This power potentially overlaps with the mandate of the foreign intelligence service of Ukraine (SZR).[162] Furthermore, such a formulation implies that SSU officers are potentially allowed to operate abroad. **The Draft Law should clarify how would SSU's mandate complement SZR's field of work and how overlaps would be avoided to secure the proper use of state's**

[159] ibid. Practices 28 and 30 (2010 UN SRCT Compilation).
[160] ibid. Practices 28 and 30 28 (2010 UN SRCT Compilation).
[161] ibid. Practice 28 (2010 UN SRCT Compilation).
[162] For SZR's mandate see: https://szru.gov.ua/en/about/about-szru.

resources. The Draft Law should also be clearer about whether SSU staff is allowed to be deployed and operate abroad.

107. Article 14.3 of the Draft SSU Law provides that *"[i]nformation obtained or created by the [SSU] as the result of counterintelligence and intelligence activities may not be used to address the tasks related to criminal proceedings other than in the manner prescribed by the Law of Ukraine 'On Counterintelligence Activity'*". This provides a safeguard by attempting to separate the use of information obtained as part of counter-intelligence, and information used in the context of criminal investigations. However, the provision does not elaborate on how this separation will be regulated in practice and overseen by the respective oversight actors. **The Draft SSU Law should be supplemented in that respect**.

5.10. Other Comments

108. Article 12.1 ends by stating that *"[o]ther powers may be vested in the Security Service of Ukraine solely by law*". While it is welcome that such powers will be defined by law, this creates a potentially open-ended list of powers. This also increases the risk of having such powers scattered across several legal acts, thus blurring the exact scope of the SSU powers and potentially impacting the accessibility of the legal framework regulating the SSU. **The drafters should reconsider such a provision**.

109. Article 21 of the Draft SSU Law makes *"[l]egitimate demands/requests of the officials of the [SSU] binding on all natural and legal persons".* The provision does not elaborate on which institutions would determine whether a demand/request by an SSU official is legitimate. Without any clear 'checks' / legitimacy tests foreseen by the law, this power risks violating the rule of law principle, and may result in arbitrary practices. **The drafters should introduce a mechanism for assessing the legitimacy of such requests.**

6. MONITORING AND OVERSIGHT OVER THE ACTIVITIES OF THE SECURITY SERVICE OF UKRAINE

110. Section VII of the Draft SSU Law regulates the monitoring and oversight mechanisms of the SSU activities, which range from democratic civilian oversight (Article 45) to control/oversight by the President (Article 46), the Parliament (Article 47), financial audit (Article 48), judicial oversight (Article 49), internal monitoring and oversight (Article 50), public engagement in oversight (Article 51) and supervision of the observance of law by the prosecution (Article 52). Having a multilevel system of internal, executive, parliamentary, judicial, specialized and public oversight mechanisms is generally in line with international recommendations.[163]

111. As the below analysis shows, however, for most of the oversight actors, the Draft SSU Law does not really elaborate the mandates and powers of the overseers, and instead leaves it to a future law to be adopted. Moreover, in most cases, the oversight actors seem to be limited to monitoring the legality of the SSU acts, and not other aspects of SSU's work as recommended by the *UN SRCT Compilation*.

[163] *Op. cit.* footnote 5, Practice 6 (2010 UN SRCT Compilation); page 58 (2015 CoE Commissioner for Human Rights *Democratic and Effective Oversight of National Security Services*); par 7 (2015 Venice Commission's *Report on the Democratic Oversight of the Security Services)*; and page 28 (2017 EU FRA Surveillance by Intelligence Services). See also the 1994 *OSCE Code of Conduct on Politico-Military Aspects of Security*, whereby OSCE participating States "*consider the democratic political control of military and paramilitary forces as well as the activities of the internal security and intelligence services to be an indispensable element of stability and security*"(par 20).

112. Article 45 of the Draft SSU Law outlines the general principles of overseeing the SSU. Article 45.2 stipulates that oversight of the SSU will be carried out by "*authorized bodies and officials*". **This provision could explicitly, at the outset, name the whole range of bodies and persons mandated with the oversight of the SSU, though in a non-exhaustive manner, in view of additional oversight bodies/mechanisms that may be set-up in the future**. Second, **a list of actors mandated to oversee should not be limited to "state-authorized bodies" and should also include the civil society, media, and the general public**, who are legitimately entitled to bring SSU's actions under public scrutiny. These non-state actors may act more as a "watchdog" since they do not have the formal authority and mechanisms to hold SSU to account. However, they clearly play a crucial role in uncovering violations, fostering informed public debate, and instigating key litigation (see also Sub-Section 6.5 *infra*).

113. The combined remit of oversight institutions should cover all aspects of the work of intelligence services, including **their compliance with the law and international human rights standards, the effectiveness and efficiency of their activities, gender and diversity, their finances and their administrative practices**.[164] As such, oversight should not only focus on the "*activities of the SSU*" as stipulated, for instance, in the title of Section VII of the Draft SSU Law but all such aspects of the SSU's functioning and work. **The Draft SSU Law should be amended in that respect**.

114. Articles 45.2 and 45.3 refer to the duty of oversight institutions to protect classified information and personal data, which is in line with international recommendations.[165] While this practice is necessary to protect sensitive information linked to national security, it does not mean that oversight institutions should not have autonomy on what they publish and report on. As per the Tshwane Principles, "*independent oversight institutions should give the institutions subject to their oversight the opportunity to review, in a timely manner, any reports which are to be made public in order to allow them to raise concerns about the inclusion of material that may be classified. The final decision regarding what should be published should rest with the oversight body itself".*[166] This is quite important to ensure that oversight bodies remain independent and are not unnecessarily and arbitrarily censored by the security services. In this respect the second sentence of Article 45.2 which states that "*[i]nformation obtained as the result of oversight shall be processed, stored, transmitted and/or made public in compliance with the requirements stipulated by this Law"* is not in line with the aforementioned recommendation because the Draft SSU Law allows information to be made public only upon the approval of the SSU's management (see also Articles 14.4 and 15.1 of the Draft SSU Law). **Articles 45.2 and 45.3 should be revised to ensure that independent oversight bodies, after making sure that their reports do not contain classified material or personal data, have the final say on what they publish and report to the public, without the requirement of SSU's management approval**.

115. Article 45.4 touches upon the oversight bodies' access to information and facilities. It is concerning that the provision postpones the regulation of access to information to future laws while oversight bodies' access to facilities will be regulated through secondary regulation to be adopted by the SSU. This means that until such legislation/regulation are adopted, oversight institutions may be unable to exercise their mandates in any meaningful way. International standards and recommendations emphasize that full and unhindered access to information, including classified information relevant to their functions, officials and installations is essential to oversight bodies to carry out their

[164] ibid. Practice 6 (2010 UN SRCT Compilation).
[165] ibid. Practice 8 (2010 UN SRCT Compilation).
[166] See *op. cit.* footnote 5, Principle 34 (B) 4 (2013 Tshwane Principles).

functions.[167] Principles 32-33 of the Tshwane Principles also stipulate that such access should extend to "*all records, technologies, and systems in the possession of security sector authorities, regardless of form or medium and whether or not they were created by that authority; physical locations, objects, and facilities; and information held by persons whom overseers deem to be relevant for their oversight functions"*.[168] It is also essential that all those involved in interception activities have a duty to disclose to the SSU any material it requires.[169] Also, oversight bodies should have access to the necessary financial, technological, and human resources to enable them to identify, access, and analyze information that is relevant to the effective performance of their functions.[170] An oversight body of which the functions include reviewing questions of legality, effectiveness and respect for human rights will require access to even more specific information.[171]

116. As recommended in the *ODIHR Opinion on the Draft Concept*, **all oversight bodies should have a right to access to all (classified) information relevant to their functions and necessary for discharging their responsibilities on the basis of procedure clearly defined by law, and this should be expressly stated under Section VII of the Draft SSU Law**. In view of the aforementioned international standards and recommendations, **the Draft Law should regulate such access to information and to the premises of the SSU under Section VII and provide oversight institutions with unfettered access to information, officials, premises and records/documents/technologies and systems in SSU's possession instead of leaving this for future legislation/regulation.** In support of oversight bodies **the SSU should be obliged to keep detailed records and to disclose to oversight bodies any material requested.**[172] **This should be reflected in Article 45 of the Draft SSU Law.**

6.1. Control by the Executive

117. Article 46.1 of the Draft SSU Law provides for President's control over SSU activities both directly and through the National Security and Defence Council and other subsidiary bodies. In addition, Article 46.2 provides that officials specially designated by the President will scrutinize the legality of SSU regulations as well as monitor the legality of SSU's surveillance functions. In order to ensure that the scope of the executive control sufficiently covers the scrutiny of SSU regulations and activities' compliance with the law and international human rights standards, and to prevent overlaps among the various bodies (NSDC and subsidiary bodies) and individuals, **Article 46 should clearly stipulate the respective control mandate of those executive actor**s. If the mandate of the "designated individuals" will be determined by regulations, **such secondary legislation should be public**. Ideally, **those designated individuals should serve as Inspector-General/Commissioner with the mandate to carry out inspections and investigations on behalf of the executive into alleged violations of the law and human rights, and refer cases to the judiciary where necessary**.[173]

---

[167] See e.g., ECtHR, *Roman Zakharov v. Russia* [GC] (Application no. 47143/06, judgment of 5 December 2015), par 281; par 98 (2015 Venice Commission's *Report on the Democratic Oversight of the Security Services)*; *op. cit.* footnote 5, Practice 7 (2010 UN SRCT Compilation); Principles 6 and 32-33 (2013 Tshwane Principles); and pars 49-50 (2015 CoE Commissioner for Human Rights *Democratic and Effective Oversight of National Security Services*).

[168] See *op. cit.* footnote 5, Principle 32 (B) (2013 Tshwane Principles).

[169] ECtHR, *Roman Zakharov v. Russia* [GC] (Application no. 47143/06, judgment of 5 December 2015), par 281.

[170] *Op. cit.* footnote 5, Principle 33 (2013 Tshwane Principles).

[171] See e.g., Venice Commission, *2007 Report on the Democratic Oversight of the Security Services*, par 163.

[172] See e.g., European Parliament, *Resolution on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs*, adopted by the European Parliament on 12 March 2014 (2013/2188(INI)).

[173] *Op. cit.* footnote 5, par 147 (2007 Venice Commission's *Report on the Democratic Oversight of the Security Services)*, where the Venice Commission states that the function of an Inspector-General strengthens executive control and can also assist the work of external oversight bodies, in particular parliamentary oversight and other expert bodies.

118. Article 46.3 stipulates that the SSU will regularly inform the President, NSDC, and designated individuals on the violations of the law. It appears rather unrealistic to expect any security service to regularly and proactively report on violations of the law to their superiors. It is therefore important that these "*specially designated individuals*" appointed by the President have strong and broad mandate to monitor compliance with the law, handle complaints/internal whistleblowing and conduct investigations on behalf of the executive, as done in some other countries.[174] Generally, the executive supervises intelligence services in a variety of ways, e.g., by establishing their policies, priorities or guidelines; by nominating and/or appointing the service's senior management; by being involved in the process of authorizing specific surveillance measures; or by approving co-operation with other services.[175] **To clarify more explicitly the scope of the control by the executive, these aspects could be outlined as appropriate under Article 46 of the Draft SSU Law**.

6.2. Parliamentary Oversight

119. Article 47.1 of the Draft SSU Law refers to parliamentary oversight by the Verkhovna Rada of Ukraine (in terms of law-making concerning the regulation of the activities of the SSU, its powers, budget and reporting). Paragraph 3 specifies that such oversight functions are performed by the Parliamentary Committee of the Verkhovna Rada controlling the activities of special purpose bodies. In addition, the Parliament Commissioner for Human Rights of the Verkhovna Rada is in charge of overseeing the observance of constitutional rights, human and civil rights and freedoms by the SSU.

120. It is good practice that a Parliamentary Committee of the Verkhovna Rada is mandated to oversee the SSU.[176] **At the same time, Article 47.3 should further elaborate on its oversight mandate in relation to specific aspects of the work of security services, such as overseeing information collection measures, co-operation and information exchange with foreign services, the use of personal data, as well as the handling of individual complaints against security services** as recommended in the *UN SRCT Compilation*.

121. At the same time, operational oversight is time-consuming and requires extensive powers of access and substantial time, human and financial resources, not to mention technological expertise to oversee the most technical and complex aspects of the security/intelligence work such as mass surveillance, signals intelligence and so forth. Therefore, the designated parliamentary committee may benefit from the use of external and independent experts, or even to establish a separate (independent) expert body exclusively dedicated to overseeing security services with extensive oversight powers, as increasingly done for instance in the EU.[177] Such expert bodies generally have powers such as authorizing surveillance measures, investigating complaints, requesting documents and information from the intelligence services, and/or giving advice to the

---

[174] For example, in the United Kingdom, the Prime Minister appoints two Commissioners in charge of overseeing the intelligence services; see United Kingdom, *Regulation of Investigatory Powers Act* (2000), Sections 57(1), 59(1).

[175] See EU FRA, *Surveillance by Intelligence Services*, Vol 2, (2017), page 60.

[176] *Op. cit.* footnote 5, par 15d (2005 PACE Resolution 1713), which states that "*the control of activities of special services should be carried out by a special parliamentary committee"*.

[177] Among those European countries, Germany and Belgium have set-up powerful expert oversight bodies, namely the G-10 Committee in Germany and the Standing Intelligence Oversight Committee (Committee I) and Administrative Commission in Belgium. The Committee I in Belgium (i) reviews and provides advice on laws, or any other policy documents relating to the governance of security services, while also providing written advice to the judicial authorities on the legality of the way in which information added to criminal proceedings was collected by the intelligence and security services; (ii) conducts ex-post oversight of the implementation of targeted surveillance measures, while the Administrative Commission is in charge of ex-ante authorisations; (iii) oversees strategic surveillance conducted abroad by the military intelligence agency and also oversees the security services' cooperation with their international counterparts, which is a novel approach among expert oversight bodies; (iv) upon complaints, requests by the Parliament or judicial authorities, carries out investigations, including investigations against members of the services who are suspected of having committed a felony or misdemeanour, in a judicial capacity; and (v) serves as an appeal body for security clearances (see <https://www.comiteri.be/index.php/en/standing-committee-i/eight-assignments>). See also *op. cit.* footnote 5, page 68, Table 2 (2017 EU FRA Surveillance by Intelligence Services).

executive and/or parliament. **The legal drafters may consider whether the designated parliamentary committee has sufficient time and resources to discharge its oversight functions and whether such tasks should be delegated to a separate expert body.**

122. It is welcome that Article 47.2 provides that the Verkhovna Rada "*may formally invite or summon officials (officers) of the Security Service of Ukraine to report at a plenary session*". **The power to summon officials should also be given to the dedicated parliamentary committee, so that they can have a closed session to discuss matters relating to SSU activities in details**. This may prove more effective than only summoning the SSU officers on a plenary session whereby sensitive information cannot necessarily be shared with the entire parliament. Moreover, such a provision is unlikely to be complied with if not accompanied with **sanctions in case of non-compliance**[178] and **this should be added in Article 47.2 of the Draft SSU Law.**

123. Moreover, for parliamentary oversight to be effective, the parliamentary committee should be granted additional powers which should be explicitly mentioned in the Draft SSU Law, unless provided in another legislation or rules of procedure of the Verkhovna Rada, in which case a cross-reference should be made to the said legal text(s). **These should include the ability to launch parliamentary investigations on its own initiative; to conduct inspection of SSU facilities; to receive and handle complaints, investigate them and issue recommendations or binding decisions; and/or being involved in the authorization process of surveillance measures**.[179] The legal drafters could also consider giving the designated parliamentary committee the powers **to receive and hear protected disclosures from whistle-blowers**, as is for instance the case for Belgium's expert oversight body, which reports to the parliamentary committee.[180]

124. Article 46 should also **further elaborate on parliament's power and authority to make public interest disclosures**. As per the Tshwane Principles, "*the legislature should have the power to disclose any information to the public, including information which the executive branch claims the right to withhold on national security grounds, if it deems it appropriate to do so according to procedures that it should establish"*.[181] This would mean that democratically elected parliamentarians cannot be censured by the security services on the grounds of public security, if the parliamentary committee concludes that there is a greater public interest in disclosing certain information.[182]

125. Parliamentary access to classified information is a key power to perform parliamentary oversight functions and unhindered access to information should be particularly emphasised for parliamentary oversight bodies. A recent survey carried out by the NATO Parliamentary Assembly mapped out member state practices, and found that a great majority of NATO member states grant either all parliamentarians or selected parliamentary committees with access to classified information; furthermore, in two thirds of the surveyed countries, parliamentarians sitting in security-relevant committees do not undergo security vetting.[183] **The drafters may benefit from taking into consideration such international good practices and consider providing similar**

---

178 See e.g., *op. cit.* footnote 5, par 14 (2010 UN SRCT Compilation).

179 *Op. cit.* footnote 114, pages 34-35 (2017 EU FRA Surveillance by Intelligence Services); and page 35 (2015 EU FRA's *Mapping of legal frameworks on Surveillance by Intelligence Services within the EU*).

180 ibid. page 27 (2015 EU FRA's *Mapping of legal frameworks on Surveillance by Intelligence Services within the EU*).

181 *Op. cit.* footnote 5, Principle 36 (2013 Tshwane Principles).

182 This is for instance the case in the United Kingdom where the reports of the Parliament's Intelligence and Security Committee, whether annual or *ad hoc*, usually contains redactions on security grounds suggested by the services – but these must be justified, and the committee has the final say; see *op. cit.* footnote 5, page 88 (2017 EU FRA Surveillance by Intelligence Services).

183 See NATO Parliamentary Assembly-DCAF, Yildirim Schierkolk, Nazli, *Parliamentary Access to Classified Information* (2018), pages 22-26..

modalities concerning access by parliamentarians or committee members to state secret and classified information.

126. **It is also important that parliamentary oversight be gender- and diversity-sensitive and this could be expressly stated in Article 47**. This means that the parliament should ensure that security needs are defined in an inclusive manner and that laws and regulations concerning security address diverse needs, that gender and diversity are mainstreamed for the security sector and parliamentary oversight is diverse and inclusive. In that respect, the *2019 DCAF-OSCE/ODIHR-UN Women Tool no. 7 on Parliamentary Oversight of the Security Sector and Gender* can serve as a useful reference tool.

127. Finally, Article 47.4 provides that parliamentary oversight over the SSU's observance of constitutional rights, human and civil rights and freedoms shall be exercised by the Ukrainian Parliament Commissioner for Human Rights. At the same time, as is the case for other oversight actors, **Article 47.4 does not elaborate the mandate and powers of Parliament Commissioner for Human Rights in overseeing the SSU and should be supplemented in that respect** taking into account the aforementioned recommendations also reflected in Practice 7 of the *UN SRCT Compilation*.[184] Especially, **if the designated parliamentary committee is not empowered to receive and handle complaints from individuals, then the Parliamentary Commissioner for Human Rights should be mandated to do so. It would also be advisable to make clear in Article 47 of the Draft SSU Law what the relationship of the Commissioner is to the designated parliamentary committee, in order to prevent gaps in oversight**.[185]

6.3. Judicial Oversight

128. As mentioned above, the Draft SSU Law does not always clarify which SSU activities require a court order or another form of authorization from the judiciary. Article 49 of the Draft SSU Law provides that *"[d]ecisions, acts or inactivity of the [SSU], its officials (officers) may be appealed in court"* and that courts shall also *"exercise oversight of enforcement of relevant court decisions*". This seems to imply that the role of courts and judges is limited to ex-post oversight and to adjudicating on cases brought before them. This is not in line with international recommendations. Indeed, PACE clearly states that *"[t]he judiciary should be authorised to exercise extensive a priori and ex post facto control"* over intelligence services.[186] This should include prior judicial authorization to carry out certain operative/investigative activities with a high potential to infringe upon human rights as well as some form of follow-up control that checks whether conditions are being complied with[187] (see also Sub-Section 5.2 *supra*).

129. **It is important that the Draft SSU Law further elaborates the scope and extent of judicial oversight, both in terms of *a priori* and *ex post facto* control. This should include in particular the authorization of surveillance, the ongoing oversight/follow-up control of information collection measures** (supervision of investigations, ordering the termination of surveillance and ordering the destruction of data collected) **and *ex-post* adjudication of cases**[188] (see also comments below on prosecution's supervision of covert and other investigative powers of the SSU). Moreover, **Article 49 should stipulate**

---

184 Practice 7 of the UN SRCT Compilation states: "*Oversight institutions have the power, resources and expertise to initiate and conduct their own investigations, as well as full and unhindered access to the information, officials and installations necessary to fulfil their mandates. Oversight institutions receive the full cooperation of intelligence services and law enforcement authorities in hearing witnesses, as well as obtaining documentation and other evidence*".

185 *The UN SRCT Compilation* states in Practices 3 and 6 that the laws covering the intelligence and security services should exhaustively cover their powers and competences and oversight institutions should together cover all aspects of the agencies' work.

186 *Op. cit.* footnote 5, par C.3 (1999 PACE Recommendation 1402).

187 See e.g., Venice Commission, *Report on the Democratic oversight of Signals Intelligence Agencies*, CDL-AD(2015)011, par 24.

188 See e.g., Venice Commission, *Report on the Democratic oversight of Signals Intelligence Agencies*, CDL-AD(2015)011, pars 105-106; ECtHR, *Klass and Others v. Germany* (Application no. 5029/71, judgment of 1978), pars 55-56 ; and *op. cit.* footnote 5, Practice 22 and par 35 (2010 UN SRCT Compilation).

who can apply to challenge the legality of SSU actions or alleged actions, the relevant procedure or court, the grounds for upholding an application or the available remedies. It is worth noting that where there is evidence that national courts merely "rubber-stamp" executive applications, the ECtHR has discounted the effectiveness of judicial *ex ante* approval.[189]

130. Finally, as regards remedies, the ECtHR has stressed that, even in the context of national security, the remedy required by Article 13 of the ECHR must be effective *in practice* as well as in law.[190] It has noted that if (as appears to be the case under the Draft SSU Law) there is no legal duty *under any circumstances* to inform an individual against whom criminal proceedings are *not* instituted that they have been subject to state surveillance, this renders judicial safeguards ineffective.[191] Regarding remedies which must be available in the context of measures which are known to the alleged victim, the ECtHR stated that **a court must be able to reject executive assertions of threats to national security that are arbitrary or unreasonable, that proceedings must be adversarial and that the court must examine whether a fair balance has been struck between the public interest and the individual's rights**.[192]

6.4. Internal Monitoring and Oversight

131. Article 50 of the Draft SSU Law state that the "*Head of the Security Service of Ukraine, their Deputies, chiefs (heads) of functional units of the Headquarters, regional offices, bodies, establishments (divisions thereof) and institutions of the Security Service of Ukraine, as well as officials authorised by them shall monitor the fulfilment of tasks set to personnel of the Security Service of Ukraine in accordance with the procedure established by law and acts of the Security Service of Ukraine*". At the same time, this seems to refer more to hierarchical controls than proper internal control contemplated by international recommendations and case law. Articles 50.1 and 50.4 make a general reference to the senior and mid management of the SSU, and gives them a general internal supervision duty. Articles 50.2 and 50.3 make references to internal budgetary controls. However internal control should go beyond budgetary concerns.

132. As stipulated by the Venice Commission, *"[i]nternal control of security services is the primary guarantee against abuses of power, when the staff working in the agencies are committed to the democratic values of the State and to respecting human rights".*[193] **Articles 49 and 50 should therefore be supplemented to stipulate in more detail mechanisms and procedures of internal control to ensure that the services operate in compliance with laws and human rights standards, with particular emphasis on internal review and authorization of surveillance measures and of other methods that infringes upon human rights, as well as more generally, to ensure compliance with human rights standards**. **It is also essential to provide for internal complaint channels and the protection of whistle-blowers as an important internal control mechanism** (see Sub-Section 2.4 *supra*).[194] In that respect, the ability to raise concerns internally without fear of reprisals is an essential component of whistle-blower protection, as recommended at the international level.[195] Where there is no such internal route

---

189 See e.g., ECtHR, *Iordachi and Others v. Moldova* (Application no. 25198/02), pars 47, 51 and 52.
190 See ECtHR, *Al-Nashif v. Bulgaria* (Application no. 50963/99, judgment of 20 June 2002), par 136.
191 ECtHR, *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria* (Application no. 62540/00, judgment 28 June 2007), pars 99-103.
192 See e.g., ECtHR, *Al-Nashif v. Bulgaria* (Application no. 50963/99, judgment of 20 June 2002), par 138.
193 *Op. cit.* footnote 5, par 130 (2007 Venice Commission's *Report on the Democratic Oversight of the Security Services*).
194 See *op. cit.* footnote 5, page 70 (2017 EU FRA Surveillance by Intelligence Services).
195 See *UN SRCT Compilation*, Principle 18, referring not only to internal procedures within the services for raising ethical concerns but also to the capacity for an independent body to investigate and take action where internal processes have proved inadequate. See also CoE *Recommendation CM/Rec(2014)7 of the Committee of Ministers to member States on the protection of whistleblowers*.

available then SSU officers may be justified in reporting their concerns externally and, exceptionally, in making them public through the press.[196]

133. There are various other key aspects of internal control, including management providing relevant direction or guidance on ethics and human rights compliance, putting in place periodic qualitative training in this respect as well as internal disciplinary mechanisms for misconduct.[197] This type of internal control can be carried out either through dedicated units, by establishing inspectorate generals and/or having ethics commissioners or staff counsellors, to whom staff can turn in confidence.[198] **It is recommended to supplement Articles 49-50 in that respect, while specifying the scope and powers of such mechanisms and ensure that they are allocated adequate human and financial resources.**

134. Article 49.5 of the Draft SSU Law refers to the "*state supervision of occupational health and safety of personnel; state technical supervision over observance of requirements of occupational health and safety legislation; fire safety, sanitary and epidemiological control*" carried out by the Headquarters or specially designated personnel. As further elaborated in par 12 *supra*, **it is essential that there are also proper internal complaints mechanisms regarding sexual or other abuses, violence, bullying, sexual or other harassment and other human rights violations and this should be explicitly mentioned in Article 49.5**.

6.5. Public Oversight and Transparency

135. Article 51 of the Draft SSU Law provides for "*public engagement in exercising democratic civilian oversight of [SSU] activities*" in accordance with the procedure established by the Constitution and laws, and subject to the restrictions established by the Draft SSU Law. **It is not clear what this means and should be clarified**.

136. Article 51.2 regulates how the SSU informs the public and handles requests for access to public information. First, it is worth emphasizing that refusal of information requests should not be completely left to the discretion of the Head of the SSU, as is currently the case. Moreover, the provision does not determine its terms nor establish a clear procedure for applying for such information or for dealing with refusals on access, which is not in line with international recommendations.[199] This provision also does not make reference to the relevant access to information legislation. It is good practice to have security services not completely exempted from such access to information legislation though some narrowly described exceptions and restrictions, for the purposes of protecting national security, may nevertheless apply.[200] However, **such restrictions should be strictly limited and accompanied by adequate safeguards against abuse, including**

---

196 See ECtHR, *Bucur and Toma v. Romania* (Application no. 40238/02, judgment of 8 January 2013), holding that a disclosure by a member of the Romanian Intelligence Service about unlawful interception of communications, which took the form of holding press conference, was justified in the circumstances (after he had tried to raise the matter with his superiors and with an MP). The Court concluded on the basis of a close analysis of the available avenues for raising the allegations of irregularities that none of them was likely to be effective. Moreover, the general interest in the disclosure of information revealing illegal activities within the Romanian Intelligence Service was so important in a democratic society that it prevailed over the interest in maintaining public confidence in that institution.

197 *Op. cit.* footnote footnote 5, page 58 (2015 CoE Commissioner for Human Rights *Democratic and Effective Oversight of National Security Services*); pars 132-133 (2007 Venice Commission's *Report on the Democratic Oversight of the Security Services)*; and par 15 (2015 Venice Commission's Report on the Democratic Oversight of the Security Services).

198 *Op. cit.* footnote 5, page 70 (2017 EU FRA Surveillance by Intelligence Services).

199 *Op. cit.* footnote 5, par C.5 (1999 PACE Recommendation 1402), where it is recommended that *"[i]ndividuals should be given a general right of access to information gathered and stored by the internal security service(s), with exceptions to this right in the interest of national security clearly defined by law. It would also be desirable that all disputes concerning an internal security service's power to bar disclosure of information be subject to judicial review*". See also ODIHR, *Guidelines on the Protection of Human Rights Defenders* (2014), pars 145-148.

200 See e.g., DCAF, Hans Born and Ian Leigh, *Making Intelligence Accountable: Legal Standards and Best Practice for Oversight of Intelligence Agencies* (2005), page 44.. For instance, in the EU, laws of all Member States allow for some form of limitation on the right to access to information based on a threat to national security and/or objectives of security services; see *op. cit.* footnote 114, page 62 (2015 EU FRA's *Mapping of legal frameworks on Surveillance by Intelligence Services within the EU*).

full review by the courts.[201] The *Tshwane Principles* as well as the example of Canada, which has one of the most comprehensive freedom of information legislation, could be useful in that respect.[202] If not already provided in the *Law of Ukraine on Access to Information*, provided that this Law is itself compliant with international human rights standards, **it would be advisable to specify the rules and procedures regarding access to information by the public, restrictions to access, and remedial routes against such restrictions in detail and Article 51 should include a clear reference to relevant legislation**.

137. What is also missing in Article 51 is references to the role of civil society in overseeing the SSU. The legal drafters could consider supplementing **Article 51 to introduce consultative / advisory mechanisms or platforms to engage the SSU with NGOs on draft laws and implementation of policies, and discussing challenges and ways to improve human rights protection**.

6.6. Prosecutor's Office's Supervision of Covert and Other Investigative and Detective Operations

138. Article 52.1 provides that "*supervision over the covert and other investigative actions and detective operations*" by the SSU shall be carried out by the Prosecutor General and duly authorized prosecutors "*in accordance with the procedure established by law*". It is not clear what form this supervision is to take e.g. whether this involves ex ante authorisation as well as follow-up control. **This should be clarified.**

139. At the outset, it is worth noting that international standards and recommendations require that intelligence-collection measures that impose significant limitations on human rights are authorized and overseen *by at least one institution that is external to and independent of the intelligence services*, while emphasizing that **judicial bodies are generally best placed** to conduct an independent and impartial assessment of an application to use intrusive collection powers, as well as ongoing and *ex-post* oversight.[203] It is actually an established practice, for instance in the EU, that the judiciary or an independent expert body having judicial powers is effectively involved in *ex-ante* authorization of surveillance measures, as shown for instance in a recent survey conducted by the EU Fundamental Rights Agency (FRA).[204]

140. When such supervision functions are carried out by the prosecution service, the ECtHR generally examines whether the prosecutors are independent of the authorities carrying out the surveillance, and are vested with sufficient powers and competence to exercise effective and continuous control.[205] While it goes beyond the scope of this review to determine whether the Prosecutor General presents sufficient guarantees of independence

---

[201] See e.g., *op. cit.* footnote 5, Principle 3 (2013 Tshwane Principles), which states: *'[N]o restriction on the right to information on national security grounds may be imposed unless the government can demonstrate that: (1) the restriction (a) is prescribed by law and (b) is necessary in a democratic society (c) to protect a legitimate national security interest; and (2) the law provides for adequate safeguards against abuse, including prompt, full, accessible, and effective scrutiny of the validity of the restriction by an independent oversight authority and full review by the courts*".

[202] In Canada, Articles 13-16 of the *Access to Information Act*, stipulate the exemptions from the Government's duty to disclose information. However, the same law provides in detail the procedures for appealing the government institution's decision to refuse public access to information: the Information Commissioner is entitled to receive, handle and investigate complaints regarding government institutions' refusal to give access (Articles 30-36) and based on the results of the investigation, the Commissioner issues recommendations to the government institution including appropriate actions to be taken (Article 37). If the government institution does not provide access to information despite the Information Commissioner's recommendation, the complainant can take the case to the Federal Court (Article 41), and accordingly provides strong remedies against refusal to access information, in line with international standards.

[203] See e.g., *op. cit.* footnote 5, Practice 22 and par 35 (2010 UN SRCT Compilation); and ECtHR, *Klass and Others v. Germany* (Application no. 5029/71, judgment of 1978), pars 55-56.

[204] The only exceptions are Cyprus, Malta, Ireland, Luxembourg, and France; some countries such as Germany and Sweden go one step further and subject mass surveillance (signals intelligence) also to ex-ante authorization by expert bodies with quasi-judicial powers; see *op. cit.* footnote 114, pages 52 and 55 (2015 EU FRA's *Mapping of legal frameworks on Surveillance by Intelligence Services within the EU*).

[205] See e.g., ECtHR, *Roman Zakharov v. Russia* [GC] (Application no. 47143/06, judgment of 5 December 2015), par 277.

in the Ukrainian context, it is noted that the ECtHR has found on several occasions the prosecution service to be insufficiently independent from the executive branch.[206] **The legal drafters should therefore consider transferring such supervision functions to judicial bodies instead and revise Articles 49 and 52 accordingly.**

141. In any case, the effectiveness of Prosecutor General's supervision is undermined by the important qualification in Article 52.2 of the Draft Law, which specifies the types of information that shall not be communicated to the prosecution service. This excludes not only information on the identities of SSU officers and sources (which is justifiable) but also broader questions such as methods, planning and logistics which are directly relevant to ensuring that SSU operations comply with legal, constitutional and human rights standards. Without access to such information, it is hard to see how such supervision can serve as a meaningful safeguard and **such limitations should be reconsidered and exceptions limited to protection of identities only**. Some good practice examples could serve as useful guidance.[207]

142. **To ensure an effective oversight system, it is also essential that the said oversight institution has the power to order the revision, suspension or immediate termination of surveillance measures when a violation by security services is identified**,[208] as well as **the destruction of the data collected unlawfully**.[209] **This should also be reflected in the Draft SSU Law.**

7. HUMAN RESOURCES MANAGEMENT AND LEGAL AND SOCIAL PROTECTION OF SSU PERSONNEL

143. Section IV of the Draft SSU Law regulates the recruitment, status and career of SSU personnel as well as their disciplinary and other liability. It confirms that there is a dual structure in the workforce of the agency, with civilian staff working as civil servants and personnel with 'special ranks' who are soldiers assigned to and serving in the SSU.

7.1. Recruitment of SSU Personnel

144. Article 10.4 (5) of the Draft SSU Law gives an absolute and unchecked authority to the Head of the SSU to appoint and dismiss personnel. **Appointment and dismissal should not be left to the personal prerogative of the Head of the SSU and should be regulated by clear, objective and transparent rules**. **Article 10. 4 (5) of the Draft SSU Law should therefore be substantially revised.**

145. Article 23.2 of the Draft SSU Law includes a long list of ineligibility criteria, a number of which may give rise to discrimination concerns. Article 23.2 (1) excludes persons who "*have been recognised, according to the procedure established by law, as partially capable or incapable*". This is not in line with the non-discrimination principle, as stipulated in Article 14 of the ECHR. While it may be understandable that persons with certain types of disabilities may not be eligible for certain operational positions, this does

---

[206] ECtHR, *Roman Zakharov v. Russia* [GC] (Application no. 47143/06, judgment of 5 December 2015), par 278; and *Iordachi and Others v. Moldova* (Application no. 25198/02), par 47.

[207] For instance, in Spain, the ***Spanish*** National Intelligence Centre must get permission from a Supreme Court judge when carrying out measures that target communications. When requesting such authorisation, the Spanish National Intelligence Centre has to provide information on the specific nature of the measures; articulate the facts, purposes and reasons underlying the adoption of such measures; identify the person/s who will be affected by the surveillance measure, if they are known; and specify the duration of the requested measures'; see *op. cit.* footnote 114, page 54 (2015 EU FRA's *Mapping of legal frameworks on Surveillance by Intelligence Services within the EU*).

[208] ECtHR, *Roman Zakharov v. Russia* [GC] (Application no. 47143/06, judgment of 5 December 2015), par 282; and *op. cit.* footnote 5, Practice 22 (2010 UN SRCT Compilation).

[209] ibid. ECtHR, *Roman Zakharov v. Russia* [GC] (Application no. 47143/06, judgment of 5 December 2015), par 168 ; and Practices 24-25 (2010 UN SRCT Compilation).

not justify excluding all persons who have been recognized as "partially capable or incapable" from working within the SSU. It is also worth referring to the recommendations made by the CRPD in its latest *Concluding Observations* on Ukraine (2015), whereby it expressed concerns "*about the lack of employment opportunities for persons with intellectual and psychosocial disabilities and the absence of policies or programmes for supported employment in the open labour market*" and called upon Ukraine to ensure effective implementation of affirmative measures and strengthen incentives for businesses and the public sector to employ persons with disabilities. The same line of argument is also applicable to Article 23.2 (2), which excludes candidates having "*medical conditions that impede their performing relevant official duties*" without defining neither the medical conditions nor the "relevant official duties" and which may therefore be open to arbitrariness. **It is recommended to remove from or substantially revise ineligibility criteria under Article 23.2 of the Draft SSU Law.**

146. Articles 23.2 (4) and (7) make an applicant ineligible if they are dismissed from their previous posts due to disciplinary offences. If the dismissal is solely based on disciplinary proceedings (without any criminal or administrative judicial proceedings), it may potentially be excessive. It should be noted that in some jurisdictions, disciplinary proceedings in workplaces lack effective procedural safeguards for the accused, and the final decision is often left to the senior management without effective appeal mechanisms. In such cases, ineligibility due to dismissal from previous job on disciplinary grounds would be disproportional. **Applicants' previous work history (including disciplinary proceedings against them) can well be part of the background checks, however it should not be a reason to bar persons from applying**.

147. Article 23.4 of the Draft SSU Law refers to applicants having to undergo a vetting process, which is standard practice before recruiting persons to security/intelligence services. To avoid arbitrary application and potential unequal treatment between candidates**, the law should provide information on categories and types of information that will be collected and reviewed during the vetting process**. This could also include screening against previous misconduct in the workplace including sexual harassment and/or abuse. Furthermore **the Draft SSU Law should also regulate procedures when a candidate's application is rejected based on the results of security vetting. In such cases, applicants should be able to appeal that decision**.[210]

148. Article 23.7 of the Draft SSU Law refers to acts regulating recruitment procedures. **To enhance the openness and transparency of the SSU, it is advisable to explicitly state that such acts shall be available to the public.**

149. Article 24 refers to the appointment and dismissal of the SSU staff (excluding the Head of the SSU). The article gives broad discretionary powers to the Head of the SSU in dismissing staff. The President's concurrence is provided only in dismissing most senior management staff. For the rest of the staff, the Head of the SSU is the one and only authority. **It would be advisable to involve an internal board to conduct disciplinary actions and reach a conclusion whether a person should be dismissed or not, while ensuring that the composition of such board is diverse and gender-balanced**. This way, decision-making is more formalised and the power is not single-handed, which may increase the risk of potential bias or abuse.

150. Article 31 regulates conditions for dismissal of SSU 'special ranks' personnel. The concerns regarding non-discrimination in Article 23 (see above) are also valid for this

[210] For instance, in Belgium**,** the Council of state and Court of First Instance are competent to adjudicate on such appeals (see <https://www.comiteri.be/index.php/en/44-pages-bo-en/149-what-are-the-disputes-that-fall-within-the-competence-of-the-appeal-body>).

provision, especially in relation to "*medical conditions*", "*results of vetting*", "*double citizenship*" and "*results of disciplinary proceedings*".

7.2. Human Resources Management

151. While the Draft Concept explicitly mentioned the "*creation of equal opportunities in the recruitment and promotion of men and women and representatives of different ethnic groups and different regions of Ukraine*", the Draft SSU Law is silent in that respect. As stated in *ODIHR Opinion on the Draft Concept*, this should even be broader and not only address women and ethnic minorities, but also persons with disabilities and other under-represented persons or groups. It is important that **such a principle concerning gender- and diversity-sensitive recruitment and promotion is explicitly mentioned in Section IV of the Draft SSU Law, while in addition specifying some of the modalities to realize such an objective**. This could consist of **introducing a mechanism to ensure that the relative representation of women and men within the SSU and related branches/operative units, as well as of under-represented persons or groups, especially minorities and persons with disabilities, including in managerial positions, is taken into consideration when ranking candidates for recruitment and promotion**. For instance, in case of a tie between two candidates applying for a position, the drafters could specify that the individual belonging to the underrepresented gender or persons within the SSU/relevant branch/unit or at managerial positions, should be chosen. **If such an option is introduced, the Draft SSU Law should also include provisions pertaining to the consequences of the violation of this gender and diversity balance requirement**.[211] The recent UK Intelligence and Security Committee's 2018 *Report on Diversity and Inclusion in the Intelligence Community* can also serve as useful guidance in that respect.

152. Also and while maintaining the principle of confidentiality of individual candidates, **it would be advisable that in its annual report, the SSU includes data regarding the number of applications, including for managerial positions, information on candidates at each stage of the selection/nomination process, all of them disaggregated by gender and other information on under-represented groups**. The drafters could also state in the Draft SSU Law that **the SSU should adopt relevant policies on gender and diversity, while equally ensuring the quality of the selected candidates**.

153. Changing the recruitment and promotion modalities is not itself enough and should be accompanied by other measures to create a work environment that supports and fosters diversity and ensure gender- and diversity-sensitive working methods and practices.[212] It is essential that human resources policies address the specific needs of women, parents and care-takers, **including by providing for appropriate entitlements and parental leave,[213] and this should be reflected in the Draft SSU Law or other legislation**. A good international practice, in that respect, is the one introduced by the newly adopted *Directive (EU) 2019/1158 of the European Parliament and of the Council of 20 June 2019* on work-life balance for parents and carers, to be transposed by 2 August 2022,

[211] For instance, the Draft Amendments could provide that the selection of the candidates of the over-represented gender shall be annulled. See e.g., Article 75 of the *French Law on Equality between Men and Women* (2014). See also 2013 *Report of the UN Working Group on the issue of discrimination against women in law and in practice* (A/HRC/23/50), adopted on 19 April 2013, par 39.

[212] *Op. cit.* footnote 5, page 12 (2019 DCAF-OSCE/ODIHR-UN Women Tool no. 14 on Intelligence and Gender).

[213] ibid. page 24 (2019 DCAF-OSCE/ODIHR-UN Women Tool no. 14 on Intelligence and Gender).

which provides that "*each worker has an individual right to parental leave of four months*", irrespective of their gender.[214]

154. Moreover, as mentioned in par 12 *supra*, this also means providing for measures to ensure, an environment that is free from all forms of gender-based discrimination, harassment, including psychological and sexual harassment, and harassment and discrimination based on a staff's sex, or national or ethnic background or disability, or any other grounds.[215]

155. As mentioned in the *ODIHR Opinion on the Draft Concept*, it is important to ensure the professionalism and ethical behaviour of SSU personnel. It would be advisable **to provide in the Draft SSU Law for the development and implementation of code of ethics / code of conduct in line with international standards, which should serve as an additional guidance for internal control**.

156. Finally, it is also important that all staff members, from senior management to administrative and service staff, are required to participate in training on international human rights law and standards, gender sensitivity, sexual harassment, women's rights, rights of minorities, rights of persons with disabilities and non-discrimination as well as practical implementation of professional and ethical codes of conduct in their daily work.[216] **Article 36 of the Draft SSU Law should be supplemented in that respect**.

7.3. Human Rights and Freedoms of SSU Personnel

157. Apart from a reference to personal data protection of SSU staff (Articles 15.4 and 15.5). nothing else is said in the Draft SSU Law about the human rights and freedoms of SSU personnel, which is unfortunate. In that respect, the 1994 *OSCE Code of Conduct on Politico-Military Aspects of Security* states that *"[e]ach participating State will ensure that military, paramilitary and security forces personnel will be able to enjoy and exercise their human rights and fundamental freedoms as reflected in CSCE documents and international law, in conformity with relevant constitutional and legal provisions and with the requirements of service*".[217] Restrictions on the human rights and fundamental freedoms of the security personnel may be provided when this is contemplated by international human rights standards and providing that such restrictions are prescribed by law and necessary in a democratic society. **It would be advisable to explicitly recognize the human rights and fundamental freedoms of SSU employees under Section IV of the Draft SSU Law, while specifying that any restriction shall be strictly necessary and proportionate to ensure the political neutrality and impartiality of the public officials concerned and the proper performance of their duties**.[218]

---

[214] See *Directive (EU) 2019/1158 of the European Parliament and of the Council of 20 June 2019 on work-life balance for parents and carers*,,, Article 5, with most of its provisions to be transposed in national legislation by 2 August 2022. See also, regarding parental leave of EU offocials, Article 42a of the *Regulation (EU, Euratom) No 1023/2013 of the European Parliament and of the Council of 22 October 2013 amending the Staff Regulations of Officials of the European Union and the Conditions of Employment of Other Servants of the European Union*.

[215] See e.g., *op. cit.* footnote 5, page 24 (2019 DCAF-OSCE/ODIHR-UN Women Tool no. 14 on Intelligence and Gender).

[216] As a comparison – for NHRI, see ibid. page 87.

[217] See 1994 *OSCE Code of Conduct on Politico-Military Aspects of Security*, par 32.

[218] See e.g., on the political neutrality of public servants in general, ECtHR, *Ahmed and Others v. United Kingdom* (Application no. 22954/93, judgment of 2 September 1998), pars 53 and 63; and *Briķe v. Latvia* (Application no. 47135/99, decision of 29 June 2000). Article 22.2 of the ICCPR and Article 11.2 of the ECHR allows restrictions to be placed by states on the free association of police and members of the armed forces (and the state administration for the ECHR). See ODIHR-Venice Commission, *Joint Guidelines on Freedom of Association* (2014), par 144, where ODIHR and the Venice Commission have specifically acknowledged the possibility of imposing restrictions on the exercise of the right to freedom of association of some public officials in cases "*where forming or joining an association would conflict with the public duties and/or jeopardize the political neutrality of the public officials concerned*". At the same time, a complete ban on forming and joining a trade union would be considered to encroach on the very essence of freedom of association and as such be violating international human rights standards (see e.g., concerning military personnel ECtHR, *Adefdromil v. France* (Application no. 32191/09, 2

158. **It is also important that the Draft SSU Law elaborates certain guarantees in that respect**. This means for instance providing for the setting up of legal and administrative procedures and mechanisms to protect their rights. This is important for good governance in the security sector but also because security officials are more likely to uphold the law and respect human rights and freedom of individuals if their own rights and freedoms are guaranteed and if they are themselves treated with dignity by their superiors, their employers and the public.

159. Article 5.1 (8) of the Draft SSU Law refers to the SSU's "*non-partisanship, political neutrality and independence*" and Article 26.1 (a) provides that it is prohibited for SSU personnel to "*engage in political activities, hold membership of political parties or act on their behalf*". SSU personnel are rights-holders and restrictions to their rights and freedoms should be strictly necessary and proportionate to ensure their political neutrality and impartiality and the proper performance of their duties. The partisan political participation and party membership of certain classes of public officials may be regulated or denied in order to ensure their impartiality and the proper functioning of their non-partisan public offices, and that they are able to fulfil their public functions free of a conflict of interest.[219] Some states have adopted specific measures restricting intelligence services' involvement in party politics e.g., prohibitions on accepting instructions or money from a political party, or from acting to further the interests of any political party.[220] The ECtHR has considered that a prohibition for members of security services from joining any political party or taking part in various forms of public protest did not amount to a violation of Article 11 of the ECHR.[221]

160. However, it is unclear what "*engag[ing] in political activities*" exactly means and it could be understood in an overbroad manner, potentially limiting their freedom of expression and freedom of association, beyond what may be required to ensure their impartiality and the proper functioning of their non-partisan public offices. **It is recommended to remove or clarify such a wording, to ensure that it cannot be interpreted to unduly restrict the rights to freedom of expression and of association**.

161. It is also good practice to explicitly set legal limits to what the intelligence agencies can be asked to do, for instance **prohibiting them from using their powers to target lawful political activity or other lawful manifestations of the rights to freedom of association, peaceful assembly and expression**.[222] International recommendations also

October 2014), pars 55 and 60; and *Matelly v. France* (Application no. 10609/10, 2 October 2014), pars 71 and 75; see also European Committee of Social Rights, *CGIL v. Italy*, complaint 140/2016, decision of 7 June 2019 on the rights of members of the financial guards, who have military status, to establish and join trade unions (Article 5), to negotiate collective agreements (Article 6§2) and to strike (Article 6§4 - the decision confirming the necessity and proportionality requirement). As to political activities and membership in a political party, the *OSCE/ODIHR-Venice Commission Guidelines on Political Party Regulation* (2011) specifies that "*partisan political participation and party membership of public officials may be regulated or denied in order to ensure that such persons are able to fulfil their public functions free of a conflict of interest*" (par 117). On the political passive (standing up for election) and active (right to vote) aspects of political participation of military personnel, see also ECtHR, *Etxeberria and Others v. Spain* (Application nos. 35579/03, 35613/03, 35626/03 and 35634/03, judgment of 30 June 2009), par 50; *Davydov and Others v. Russia* (Application no. 75947/11, judgment of 30 May 2017), par 286; *Ždanoka v. Latvia* [GC] (Application no. 58278/00, judgment of 16 March 2006), par 115; and *Melnitchenko v. Ukraine* (Application no. 17707/02, judgment of 19 October 2004), par 57. As to the right to freedom of religion or belief, it may be legitimate for a state to impose on civil servants, on account of their status, a duty to refrain from any ostentation in the expression of their religions or beliefs in public (see e.g., ECtHR, *Pitkevich v. Russia* (Application no. 47936/99, decision of 8 February 2001). As such, limiting the manifestation of religion or belief during the exercise of their public functions and in other situations that are linked to one's work may be justifiable given the need for neutrality and impartiality; however, this should not be interpreted as limiting their right to manifest their religions or beliefs outside of work, in worship, teaching, practice and observance, under Article 18 of the ICCPR, so long as this does not question their neutrality and impartiality. As to freedom of expression, any individual's right to freedom of expression may be limited, as outlined in Article 19(3) of the ICCPR, if such restrictions are provided by law, are necessary out of respect of the rights or reputations of others, or in order to protect national security, public order (*ordre public*), or public health or morals, and are proportionate to such aims. Legitimate restrictions of public servants primarily derive from the principle of confidentiality, binding them to professional secrecy with regard to information obtained in the course of their functions and to the need to maintain the neutrality of the service.

219 See e.g., OSCE/ODIHR-Venice Commission, *Guidelines on Political Party Regulation* (2011), pars 117-118.

220 *Op. cit.* footnote 5, par 19 (2010 UN SRCT Compilation).

221 See e.g., ECtHR, *Rekvényi v. Hungary* (Application no. 25390/94, judgment of 20 May 1999).

222 ibid. Practice 13 and par 20 (2010 UN SRCT Compilation); and par 150 (2015 Venice Commission *Report on the Democratic Oversight of the Security Services*).).

suggest that **national law should prohibit intelligence services from acting to promote or protect the interests of any particular political, religious, linguistic, ethnic, social or economic group.**[223] **The drafters could consider introducing provisions to that effect in the Draft SSU Law**.

162. Article 26.1 (2) prohibits SSU personnel from taking part "*in strikes and other actions that impede the proper operation of public authorities and the performance of official duties*". However, in principle, the right to strike may be restricted or prohibited only for public servants exercising authority in the name of the State[224] and not all public servants, especially those exercising more administrative tasks. **The drafters should therefore review, in consultation with the social partners, various categories of the SSU personnel with a view to identifying those that may fall outside of this narrowly interpreted category.**

7.4. Disciplinary and Other Liability of SSU Personnel and Employees

163. Several provisions of the Draft SSU Law refer to the responsibility of the SSU (Article 5.1 (7)) or to the disciplinary liability of SSU personnel or employees (see e.g., Articles 10.4 (8) and 28.2 of the Draft SSU Law). Overall, the judicial accountability of SSU personnel is not dealt with clearly and comprehensively in the Draft SSU Law, neither with respect to the rules and procedures that serve to prevent unacceptable practices, nor with respect to the mechanisms that would enable such practices to be detected and perpetrator held to account.

164. Article 28.2 of the Draft SSU Law states that the grounds and procedure for disciplining SSU personnel and employees "*shall be determined by the Disciplinary Charter of the Security Service of Ukraine, which is approved by law*". While it is welcome that this will be clarified in another document approved by law, it may be advisable to set the broad principles in the SSU Law. The *UN SRCT Compilation* recommends that *"[n]ational laws provide for criminal civil or other sanctions against any member, or individual acting on behalf of an intelligence service, who violates or orders an action that would violate national law or international human rights law. These laws also establish procedures to hold individuals to account for such violations*".[225] **The Draft SSU Law should be supplemented by a clear statement that SSU personnel incur liability for violation of criminal, administrative and civil law, and international human rights law and include clear rules and procedures to prevent and detect unacceptable practices**.

165. Article 35.2 of the Draft SSU Law gives a number of privileges to SSU staff who are suspects in criminal proceedings. The last two paragraphs of Article 35.2 seem to contradict one another. There is no reasonable ground as to why SSU staff cannot be escorted, searched or detained by competent judicial/criminal justice authorities. Such privileges put SSU staff effectively above the law, and could pave the way for impunity. **It is thus recommended to remove them entirely from the Draft SSU Law**.

166. One of the issues is that according to Article 10.4 (8) of the Draft SSU Law, only the Head of the SSU is tasked with taking disciplinary actions against SSU personnel and employees. **This is problematic as this considerably limits the potential for introducing such action and should therefore be reconsidered**. It is also good practice

---

[223] *Op. cit.* footnote 5, Practice 12 (2010 UN SRCT Compilation). See also 1994 *OSCE Code of Conduct on Politico-Military Aspects of Security*, par 23; and *op. cit.* footnote 5 , par 15d (2005 PACE Resolution 1713), which states that *"[u]nder no circumstances should the intelligence services be politicized as they must be able to report to policy makers in an objective, impartial and professional manner"*.

[224] See e.g., ILO Committee of Experts on the Application of Conventions (CEACR), *Observation* - adopted 2018, published 108th ILC session (2019).

[225] *Op. cit.* footnote 5, Practice 16 (2010 UN SRCT Compilation).

for national law to require the management of intelligence services to refer cases of possible criminal wrongdoing to prosecutorial authorities.[226] **The legal drafters should consider including this aspect under Article 10 of the Draft SSU Law.**

167. In that respect, the principle of "*individual responsibility*" together with States' obligation to bring perpetrators to justice are firmly enshrined in relevant legal instruments concerning the most serious human rights violations, such as the *UNCAT* (Articles 2, 4 and 6) and the *International Convention for the Protection of All Persons from Enforced Disappearance* (Articles 6 and 23).[227] The obligations to investigate, reveal the truth, and ensure accountability, especially in anti-terrorist operations, has been noted, and is reflected in some detail at the international level, for instance in the reports of the UN Special Rapporteur on counter-terrorism.[228] This principle helps ensuring that those responsible are brought to justice, promoting accountability and preventing impunity, avoiding denial of justice and drawing necessary lessons for revising practices and policies with a view to avoiding repeated violations.[229]

168. The Venice Commission also highlights the need for establishing internal procedures to establish and trace individual responsibility for violating laws or other abuses of power.[230] Additionally, accountability also implies that superior officials shall be held responsible for the actions of persons under their command if the superior official knew or should have known of abuses but failed to take concrete action; also, public officials who refuse unlawful superior orders shall be given immunity and those who commit abuses shall not be excused on the grounds that they were following superior orders.[231] **These key principles should be explicitly stated in the Draft SSU Law**, even though they will be further elaborated in another piece of legislation.

169. Article 35.3 of the Draft SSU Law states that *"[u]njustified restriction of legitimate human rights and freedoms by personnel of the Security Service of Ukraine shall be inadmissible and punishable as stipulated by law".* **It is not clear which type of liability this would involve. It would be advisable to make a cross-reference to the relevant legislation**.

7.5. Social and Legal Protection of SSU Personnel

170. Section V of the Draft SSU Law provides measures for the "*social and legal protection*" of the SSU employees and their families. Article 37.1 provides a blanket legal protection to the SSU staff, without further stipulating the details. As mentioned in the previous sections, legal protection should not be interpreted to facilitate immunity from liability.

171. Article 37.2 provides further legal protection and includes a vague reference to the "*threat of interference with [SSU Officers] performing their duties*". Without a clear list of acts which constitutes such a threat of interference, this stipulation can be arbitrarily used to charge persons with certain offences. The Section on Final and Transitional Provisions,

---

226 ibid. par 23 (2010 UN SRCT Compilation).

227 See also Article 33 of the Rome Statute of the International Criminal Court, which was signed by Ukraine on 20 January 2000, though has yet to be ratified.

228 See e.g., UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (hereafter "UN Special Rapporteur on counter-terrorism"), *Framework Principles for Securing the Accountability of Public Officials for Gross or Systematic Human Rights Violations Committed in the Course of States-sanctioned Counter-terrorism Initiatives* (2013) A/HRC/22/52.

229 CCPR, *General Comment no. 36 on Article 6 of the ICCPR* (30 October 2018), par 27.

230 *Op. cit.* footnote 5, pars 131, 132 and 181 (2007 Venice Commission's *Report on the Democratic Oversight of the Security Services).*

231 See e.g., Article 2 of UNCAT and par 26 of the General Comment No. 2 of the UNCAT Committee; Articles 6 and 23 of the International Convention for the Protection of All Persons from Enforced Disappearance. See also e.g., the *Updated Set of Principles for the Protection and Promotion of Human Rights through Action to Combat Impunity*, recommended by the United Nations Commission on Human Rights Resolution no. 81/2005 of 21 April 2005, E/CN.4/2005/102/Add.1, Principle 27; the *UN Basic Principles on the Use of Force and Firearms by Law Enforcement Officials* (1990), Principles 24 to 26; and *UN Code of Conduct for Law Enforcement Officials* (1979), Article 5..

amends the *Code of Ukraine on Administrative Offences* and makes it a chargeable administrative offence to obstruct SSU officers from exercising their powers. There, the said acts are specified as *"[f]ailure to comply with legitimate demands of a personnel member of the [SSU], failure to provide information on the request of officials (officers) of the [SSU], providing of deliberately false or incomplete information, failure to observe statutory deadlines for providing information, obstruction of exercising statutory powers and fulfilling statutory functions by the [SSU]*". However, **it is not clear whether Article 37.2 refers to the same set of acts and this should be clarified**.

172. Article 37.4 rightfully attempts to protect the identity of SSU officers conducting undercover actions, and therefore stipulates additional data protection measures for them. However, **such withholding of information should not be applicable to overseers, especially judicial oversight mechanisms and this should be specified**.

8. Financial and Logistical Support of the Operation of the Security Service of Ukraine

173. Article 42 of the Draft SSU Law provides for the rules concerning the budget and expenditures of the SSU. Its paragraph 2 specifies that the expenditures for SSU's operational activities "*shall fall under the category of protected and classified expenditures of the State Budget of Ukraine*". The 1994 *OSCE Code of Conduct on Politico-Military Aspects of Security* stipulates that *"[e]ach participating State will, […] provide for transparency and public access to information related to the armed forces*" (par 22). **Article 42.2 raises some questions regarding the transparency of the budget process and public access to such information and the rigour of budgetary control and should be reconsidered**.

174. Article 42.1 provides that the SSU receives funding from state budget, international technical assistance and "*other sources*". The last reference opens the way for unaccounted private sources of funding separate from the state budget, which should not be allowed for transparency, good governance and accountability grounds. Funding as a part of technical assistance should be acceptable only when it is formalized in the form of a contract/agreement, which is signed or endorsed by the Executive or the Parliament, or in any case an authority above the SSU management. **Article 42.1 should be revised to remove the reference to "other sources".**

175. Further, this article states that "*Expenditures for financing the [SSU] shall amount to at least 0.45 percent of the planned gross domestic product*". The current law has no such clause, and it is not advisable to include it in the new law. By asking the Verkhovna Rada to guarantee a minimum budget allocation for the SSU, the Ukrainian government is in fact asking parliament to give up part of its budgetary powers, which might not be a good democratic governance practice, as it curtails parliament's *ex ante* control of the state budget. If, however, the government decides to include this clause in the Draft SSU Law, **it is recommended that this is based on the recorded GDP of a previous year, not an estimated future GDP.** This would provide more certainty and better transparency.

176. Article 42.2 states that the budget for SSU's operational activities will be classified as a whole. While certain parts of the SSU's operational budget may be withheld from the public to protect sensitive information necessary for the protection of national security, it is not justified to classify the entirety of the operational budget as a state secret. Regardless of its security classification, parliamentarians should be able to access, review, scrutinize and amend the SSU budget, including the parts related to its operations. **Article 42.2 should be revised accordingly, ensuring that only parts of the budget**

can be classified, yet parliamentary overseers should have access to this part in any case.

177. Article 42.5 stipulates that the procedure for financing secret operational activities should be regulated by acts and regulations of the SSU. Such SSU acts and regulations should be subject to scrutiny by external overseers, and most importantly **subject to relevant parliamentary oversight and the provision should be supplemented in that respect**.

178. Article 44 refers to the procurement processes of the SSU. Defence and intelligence procurement is an area which is prone to high risks of corruption and other misconduct. **The Draft SSU Law should stipulate in detail additional safeguards and oversight mechanisms for SSU's procurement, in addition to a regular procurement legal framework in Ukraine**.

179. To achieve the objective of a more gender- and diversity-sensitive SSU, it is also essential that adequate budget be allocated for that purpose, for instance to enhance SSU's organizational gender expertise, cover the costs associated with the establishment of a mechanism to address gender-based discrimination and harassment, or to cover maternity and parental leaves, etc.[232] **Article 42 of the Draft SSU Law could specify that these aspects are integrated in SSU's budget**.

180. Another critical stage in the budget process is the monitoring of government agencies' expenditures. Article 48 of the Draft SSU Law provides for the financial audit of the SSU by the Accounting Chamber of Ukraine (ACU), which is welcome. The Law on the Accounting Chamber stipulates that the chamber is appointed by, and accountable to, the Verkhovna Rada and that it reports regularly to the parliament. In that respect, it is welcome that Article 7.1.1 of the *Law on the Accounting Chamber* authorizes the ACU to audit secret expenditures funded by the state budget. Currently, however, auditing is limited to "*the effectiveness of the use of budget funds*" and legislation should be amended to broaden the SCU's mandate in a way that will allow it to conduct more extensive audits, e.g., including regarding the use of grants, financial and technical assistance from other states or organizations and management of state property, among others.

181. If the Accounting Chamber is to be able carry out such functions in relation to the SSU, it will need an adequate apparatus of its own as well as detailed information on the SSU's budget. It will also need necessary access to the SSU's accounting books, which should provide a clear picture of how the allocated funds have been spent. In practice, this has proved to be a challenge in certain countries.[233] **It is thus recommended to add that the SSU's accounts should be made accessible for audit by the Accounting Chamber**. **Article 48 should also be expanded to include aspects of budgetary oversight beyond an ex-post financial audit**. In doing so, this article can include a reference to the role of the parliament in ex-ante oversight (reviewing and appropriating the proposed budget of the SSU), as well as continuous and ex-post oversight (scrutinizing the expenditures and implementation of the budget).[234]

---

[232] See e.g., *op. cit.* footnote 5, Sections 33, 4.3 and 5.1 (2019 DCAF-OSCE/ODIHR-UN Women Tool no. 7 on Parliamentary Oversight of the Security Sector and Gender).

[233] In the Netherlands, for instance, the defence expert of the supreme audit authority complained about 10 years ago that the Ministry of Defence was trying to be transparent but was nonetheless difficult to audit because its bookkeeping was not clear enough.

[234] For instance, in Germany, the German Parliament has a specific parliamentary committee called the 'Trust Panel' which is exclusively tasked with overseeing the budget of security/intelligence services; the Panel has unhindered access to intelligence budgets and all relevant information, and decides on investment in surveillance technologies. See *op. cit.* footnote 114, page 37 (2015 EU FRA's *Mapping of legal frameworks on Surveillance by Intelligence Services within the EU*).

9. FINAL COMMENTS ON THE PROCESS OF PREPARING AND ADOPTING THE DRAFT AMENDMENTS

182. As mentioned in par 12 *supra* and in *ODIHR Opinion on the Draft Concept*, it is key that security policy and legislation are developed taking into consideration security needs that are defined in an inclusive, gender-responsive manner,[235] ensuring that communities and individuals participate in articulating their own needs.

183. OSCE participating States have committed to ensure that legislation will be "*adopted at the end of a public procedure, and [that] regulations will be published, that being the condition for their applicability*" (1990 Copenhagen Document, par 5.8).[236] Moreover, key OSCE commitments specify that *"[l]egislation will be formulated and adopted as the result of an open process reflecting the will of the people, either directly or through their elected representatives*" (1991 Moscow Document, par 18.1).[237] As such, public consultations constitute a means of open and democratic governance as they lead to higher transparency and accountability of public institutions, and help ensure that potential controversies are identified before a law is adopted.[238] Consultations on draft legislation and policies, in order to be effective, need to be inclusive and to provide relevant stakeholders with sufficient time to prepare and submit recommendations on draft legislation.[239] Moreover, given the potential impact of the reform, it is essential that such reform be preceded by an in-depth research and impact assessment, completed with a proper problem analysis using evidence-based techniques to identify the best efficient and effective regulatory option.[240] It is also key that proper time be allocated for the preparation and adoption of amendments.

184. In that respect, the logical sequencing is to first carry out a proper regulatory impact assessment and then develop policy document to frame the general orientations of the reform. At the time of drafting, at least three Ukrainian government documents on security matters are forthcoming, including the latest version of Ukraine's National Security Strategy (NSS), the Draft Concept on the Reform of the SSU and the Draft Amendments. If Ukraine wants its security policy to be as consistent and transparent as possible, the Ukrainian government could reconsider the timing for developing and adopting such important documents on security matters. In that respect, it would be advisable to first release and discuss the highest-level document, the NSS, and in the meantime put other security policy documents on hold. Once the NSS is adopted, the government could revisit its Draft Concept on the Reform of the SSU, to ensure that it is fully in line with the new national strategy, and release it for discussion in the Verkhovna Rada and among the public. When that process has also been completed, it will be appropriate to revisit the Draft SSU Law to ensure that it is aligned with the Draft Concept. Then the government could organize inclusive public discussions to finalize and table the new Bill on the SSU. In that respect, the fact that the Bill no. 3196 on amending the *Law of Ukraine "On the Security Service of Ukraine"* was registered with the Verkhovna Rada on 12 March, even before the adoption of the NSS and of the Concept may appear premature.

---

235 *Op. cit.* footnote 5, (2019 DCAF-OSCE/ODIHR-UN Women Tool no. 1 on SSG/SSR and Gender).
236 Available at <http://www.osce.org/fr/odihr/elections/14304http://www.osce.org/fr/odihr/elections/14304>.
237 Available at <http://www.osce.org/fr/odihr/elections/14310http://www.osce.org/fr/odihr/elections/14310>.
238 ibid.
239 According to recommendations issued by international and regional bodies and good practices within the OSCE area, public consultations generally last from a minimum of 15 days to two or three months, although this should be extended as necessary, taking into account, *inter alia*, the nature, complexity and size of the proposed draft act and supporting data/information. See e.g., ODIHR, *Opinion on the Draft Law of Ukraine "On Public Consultations"* (1 September 2016), pars 40-41.
240 See e.g., ODIHR, *Report on the Assessment of the Legislative Process in the Republic of Moldova* (2010), par 14.5.

185. Accordingly, the process by which the Draft Amendments will be developed and adopted should conform with principles of democratic law-making. Any legitimate reform process relating to the security sector, especially of this scope, **should be transparent, inclusive, extensive and involve effective consultations, including with representatives of civil society organizations and a full impact assessment including of compatibility with relevant international human rights standards. Adequate time should also be allowed for all stages of the preparation of the amendments and ensuing law-making process.** ODIHR remains at the disposal of the authorities for any further assistance that they may require in any legal reform initiatives pertaining to the judiciary or in other fields.

[END OF TEXT]