Warsaw, 13 August 2024
Opinion-Nr.: JUD-POL/509/2024 [NR/AlC]

URGENT NOTE ON JUDGES AND PROSECUTORS' ACCESS TO CLASSIFIED INFORMATION, SECURITY CLEARANCE AND RESPECT FOR JUDICIAL INDEPENDENCE AND PROSECUTORIAL AUTONOMY AND INDEPENDENCE

POLAND

This Urgent Note has benefited from contributions made by **Tamara Otiashvili**, Senior Legal Expert in International Human Rights Law and Democratic Governance; **Gar Yein Ng**, Independent Expert on Judicial Independence, Senior Lecturer in Law at the University of Buckingham, School of Law, United Kingdom and **Nazli Yildirim Schierkolk**, Independent Expert on Security Sector Reform and Human Rights;.

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

ODIHR welcomes the request for international expertise in relation to judges and prosecutors' access to classified information, and means to respect the independence of the judiciary and the prosecutorial autonomy and independence, while safeguarding national security. The Urgent Note provides an overview of relevant international and regional standards, recommendations and OSCE commitments as well as some examples of state practices with respect to the identified topics. Due to the sensitivity of the topic and diversity of state practices, the Urgent Note does not seek to be exhaustive but rather to identify relevant international human rights standards and general trends in terms of national practices to provide guidance when regulating the matter.

States may legitimately consider developing procedures or mechanisms ensuring protection of classified information. However, security clearance of judges and prosecutors, especially when carried out by an executive body, such as an intelligence or security service, may amount to or be perceived as an external influence or pressure by the executive over the judiciary and prosecution service and may therefore jeopardize judicial and prosecutorial independence. Indeed, a situation where the executive is able to control, direct or influence the judiciary is incompatible with the notion of an independent tribunal. Several soft law instruments, opinions or reports of international or regional human rights bodies as well as examples of state practices underline the inherent risks of excessive interference when having some form of security clearance of judges or prosecutors carried out by an executive body.

Consequently**, the introduction of any mechanism of security clearance of judges and prosecutors carried out by a national security service or another executive body should be discouraged in light of its potential to infringement of judicial and prosecutorial independence.** In case of security breaches or mishandling of classified information by judges or prosecutors, existing disciplinary and/or criminal procedures and sanctions, proportionate to the gravity of the offence, should be used or enhanced if necessary to more effectively address such concerns.

However, **should the legal drafters demonstrate the necessity to introduce a mechanism of security clearance for judges and prosecutors, this should be accompanied by adequate safeguards to avoid the risk of undue political influence or pressure over the judiciary and prosecution services**. Careful consideration must be given to clearly and precisely defining the personal scope of such clearance – on an *ad hoc* basis as required for the exercise of their functions or duties, as well as the nature and modalities and institutional framework to avoid a risk of arbitrary application by the public authorities and ensure there is no undue infringement upon judicial and prosecutorial independence during the security clearance process. The

requirements and procedure should be stipulated in publicly available laws, duly justified and strictly necessary and proportionate to the objective of verification, with all the safeguards to avoid a risk of the capture of the judiciary and of the prosecution in future by the political force which controls the process.

Security clearance on an ad hoc basis as required for the exercise of the judges' and prosecutors' functions or duties - To reduce the risk of undue impact on judicial and prosecutorial independence, security clearance may be considered only for those judges and prosecutors who indicate their willingness to hear cases involving classified information or when they may need to access and handle classified information when exercising judicial or prosecutorial functions or duties. To further limit the scope of security clearance, authorities may consider requiring clearance only for top-secret/secret information, and not for all levels of classified information.

Security clearance by a competent, independent and impartial body - One of the key safeguards would be to have a competent, independent and impartial body in charge of the security clearance process, such as a judicial or prosecutorial self-governing body or other independent entity, rather than an executive body or security agency, such as the intelligence or security service, directly carrying out security clearance process. The information collected by this (independent) body must be limited, both in law and in practice, to the extent that is strictly necessary for the purpose of the security clearance process. It would also be recommended to regulate, in detail in the law the key substantive and procedural safeguards to ensure its independence, namely the composition and appointment procedures of the members of the body, duration of the mandate of the members, the powers of that body, guarantees of fair trial, the decision-making rules, and the question of how the members themselves would be vetted. Even if an executive body or security service contributes to the security clearance process carried out by another (independent) body, its role in the process, both in law and in practice, must be clearly and precisely stipulated in law and limited to the extent strictly necessary for the purpose of the security clearance process. Its involvement should be minimal, not triggering the direct collection, storage and processing of a larger amount of personal data irrelevant to the purpose of security clearance and it should not have the final say in whether a judge or a prosecutor is issued security clearance or not.

Clear, precise, necessary and proportionate modalities, requirements and safeguards for security clearance - The conditions and modalities of the security clearance should be clearly and precisely defined in law to avoid a risk of arbitrary application by the public authorities, especially by the body in charge of security clearance. The requirements and procedure should also be duly justified and strictly necessary. In this respect, legislation should not be disproportionate and duplicative of existing measures aimed at ensuring judicial integrity. Moreover, the body in charge of security clearance should not have the power to unilaterally decide the withdrawal of the security clearance for allegations of no longer meeting the security clearance criteria, without proper justification and due process guarantees for the said judge, including the

possibility to challenge the withdrawal before an independent and impartial tribunal.

Mechanisms and Internal Safeguards and Measures to Ensure Security Services' Compliance with Human Rights Standards – Mechanisms and procedures of internal control and external oversight of security services should be in place to ensure that these bodies operate in compliance with laws and human rights standards and respect judicial and prosecutorial independence. The security services should ideally be subject to external oversight by an independent body with necessary mandate, powers and resources to scrutinize how security services contribute to security clearance procedures for members of the judiciary and of the prosecution service. Such measures and institutional set-up should be accompanied with specific capacity development initiatives for security/intelligence personnel to sensitize them with the importance of respecting human rights and judicial and prosecutorial independence when carrying out their functions. Relevant staff should also be provided with appropriate direction and/or guidance tools on how to carry their functions in a human rights-compliant manner.

More detailed and elaborated considerations and concrete recommendations that should be taken into account in relation to judges and prosecutors' security clearance, access to information and respect for judicial and prosecutorial independence are highlighted in the text of the Urgent Note.

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

TABLE OF CONTENTS

I. INTRODUCTION

1. On 28 May 2024, the Minister of Justice of Poland sent to the OSCE Office for Democratic Institutions and Human Rights (ODIHR) a request for expert legal advice on the topic of judges and prosecutors' access to classified information and possession of appropriate security clearance and respect for judicial and prosecutorial independence in that context.
2. On 17 June 2024, ODIHR responded to this request, confirming the Office's readiness to provide an analysis outlining applicable international and regional standards and recommendations, and where relevant, providing a comparative overview of legislative practices in other countries.
3. Given the short timeline, ODIHR decided to prepare an Urgent Note, which does not purport to be exhaustive in terms of the country practices that are referred to but attempts to provide key illustrative examples of some general patterns when addressing the issue of judges and prosecutors' access to classified information and possible security clearance or other mechanism for that purpose. The Urgent Note does not address the issue of the handling of classified information in the context of judicial proceedings and potential impact on the right to a fair and public hearing nor the issue of judicial or prosecutorial oversight over intelligence or security services.
4. ODIHR stands ready to further elaborate some of the issues addressed in the present Note, including regarding the access to and use of classified information in the context of judicial proceedings to ensure compliance with fair trial rights or judicial oversight over security services, if deemed useful to the requestor, and to review existing legislation or amendments that may be developed on the basis of ongoing discussions. Such legal reviews would provide more detailed analysis of compliance with international human rights standards and OSCE commitments and relevant examples of good practices from OSCE participating States in relation to specific legislative choices and legal provisions.
5. This Urgent Note was prepared in response to the above request. ODIHR conducted this assessment within its mandate to assist the OSCE participating States in the implementation of their OSCE human dimension commitments.[1]

II. SCOPE OF THE NOTE

6. The scope of this Urgent Note focuses primarily on the regulation of judges and prosecutors' access to classified information and possible security clearance for that purpose. It primarily aims at providing an overview of relevant international human rights standards and recommendations, OSCE commitments and good practices in the OSCE Region pertaining

1 ODIHR conducted this assessment within its mandate to assist the OSCE participating States in the implementation of their OSCE commitments. See especially *OSCE Decision No. 7/08 Further Strengthening the Rule of Law in the OSCE Area* (2008), point 4, where the Ministerial Council *"[e]ncourages participating States, with the assistance, where appropriate, of relevant OSCE executive structures in accordance with their mandates and within existing resources, to continue and to enhance their efforts to share information and best practices and to strengthen the rule of law [on the issue of] independence of the judiciary, effective administration of justice, right to a fair trial, access to court, accountability of state institutions and officials, respect for the rule of law in public administration, the right to legal assistance and respect for the human rights of persons in detention […]".*

to this topic. Thus limited, it does not constitute a comprehensive review of the legal and institutional framework regulating access to classified information by judges and prosecutors.

7. This Urgent Note raises key issues and seeks to provide general guiding principles to further pursue the contemplated reforms through the adoption of legislation, if deemed necessary. When referring to country examples, ODIHR does not advocate for any specific model; it rather focuses on providing information about applicable international standards while illustrating how they are considered in certain national laws. Any country example should be assessed with caution since it cannot necessarily be replicated in another country and should always be considered in light of the broader national institutional and legal framework, as well as country context and political culture.

8. In accordance with the Convention on the Elimination of All Forms of Discrimination against Women[2] (CEDAW) and the 2004 OSCE Action Plan for the Promotion of Gender Equality[3] and commitments to mainstream gender into OSCE activities, programmes and projects, the Urgent Note integrates, as appropriate, a gender and diversity perspective.

9. This Urgent Note does not prevent ODIHR from formulating additional written or oral recommendations or comments on the topic and other related legislation of Poland in the future. The Urgent Note is translated into Polish, but in case of discrepancies, the English version shall prevail.

III. BACKGROUND

10. The Act of 5 August 2010 on the Protection of Classified Information of Poland, as amended in April 2024,[4] regulates the classification of certain types of information the unauthorized disclosure of which would or could cause damage to the Republic of Poland or would be detrimental to its interests. Article 4 (1) of the Act provides that "*Classified information may be made available only to a person who guarantees confidentiality and only to the extent necessary to perform his work or service in the position held or to perform commissioned activities*".

11. The Act further governs the modalities for the protection of classified information, including verification procedures for granting security clearance, which may consist of ordinary verification proceedings – for positions and works related to access to classified information with the "confidential" clause (Article 25), or extended verification proceedings to access "secret" or "top secret" classified information (Article 26). According to Article 34(10)(15) of the Act, judges of common courts, military courts, the Supreme Court, administrative courts and the Supreme Administrative Court, as well as the State Tribunal and the Constitutional Tribunal, court assessors, common court jurors and military court jurors, as well as a prosecutor and a prosecutor's assistant prosecutor performing prosecutorial functions are excluded from the verification proceedings.

2 See *UN Convention on the Elimination of All Forms of Discrimination against Women* (CEDAW), adopted by General Assembly resolution 34/180 on 18 December 1979.
3 See *OSCE Action Plan for the Promotion of Gender Equality*, adopted by Decision No. 14/04, MC.DEC/14/04 (2004), para. 32.
4 See <Ochrona informacji niejawnych. - Dz.U.2024.632 t.j. - OpenLEX>.

IV. RELEVANT INTERNATIONAL HUMAN RIGHTS STANDARDS AND OSCE HUMAN DIMENSION COMMITMENTS

12. Several international human rights instruments and OSCE commitments are relevant to establish a framework for protecting fundamental rights and respecting judicial independence and prosecutorial autonomy and independence, when judges and prosecutors access and handle classified information, as well as to develop procedures and mechanisms to protect national security interests. While there is evidently a necessity to protect national security, there is however a need to ensure that security measures do not compromise core principles of justice and human dignity. Additionally, transparency, accountability, and proportionality are essential to maintain public trust and uphold the rule of law while protecting sensitive information that has been classified for necessary security reasons. Acknowledging the general tendency to make security interests prevail over the compliance with human rights standards, it is fundamental to reiterate that the protection and promotion of all human rights, and of judicial independence, as well as the protection of national security should not be seen as exclusive, but rather as complementary and mutually reinforcing objectives, an approach that also lies at the very heart of the OSCE's comprehensive concept of security.

13. In principle, information held by public authorities should be based on the principle of maximum disclosure, establishing a presumption that all such information is accessible subject only to a narrow system of exceptions,[5] including on ground of national security to protect "state secrets". To avoid over-classification, secrecy laws should define "national security" precisely and include narrowly and clearly defined prohibited disclosures, which are necessary and proportionate to protect national security; clear and transparent procedures to avoid over-classification of documents and to de-classify information no longer necessitating a higher protection on ground of national security should also be in place.[6] National security is defined in the caselaw of the ECttHR to include "…*the protection of state security and constitutional democracy from espionage, terrorism, support for*

5 See *Joint Declaration*, by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression, adopted 6 December 2004, page 2, which provides that: "*The right to access information held by public authorities is a fundamental human right which should be given effect at the national level through comprehensive legislation (for example Freedom of Information Acts) based on the principle of maximum disclosure, establishing a presumption that all information is accessible subject only to a narrow system of exceptions*."

6 See, *Interim Joint Opinion on the Draft Law of the Kyrgyz Republic on the Mass Media (as of 13 May 2023)*, ODIHR-OSCE/ RFoM 26 July 2023, para. 79; see also *Guidelines on the Protection of Human Rights Defenders*, ODIHR, 2014, para. 144. In particular, legislation should indicate clearly the criteria, which should be used in determining whether or not information can be declared secret, and therefore classified, with potentially different level of classification, so as to prevent abuse of the label "secret" for purposes of preventing disclosure of information that is in the public interest; disclosure should not be limited in the absence of the public authorities showing of *a real and identifiable risk of significant harm to a legitimate national security interest* that outweighs the public interest in the information to be disclosed; clear and transparent procedures should be put in place to avoid over-classification of documents, unreasonably long time-frames before de-classification and undue limitations in accessing historical archives; the classification of documents as secret need to be revisited on a regular basis, as information that was initially considered highly confidential may no longer fall under this category some years later; exceptions to the principle of disclosure of public information should be determined by an independent body, preferably a court, and not by the body holding the information; see UN Human Rights Committee, *General Comment No. 34* on Article 19 of the ICCPR, CCPR/C/GC/34, 21 July 2011, para. 30; International Mandate-Holders on Freedom of Expression, *2004 Joint Declaration* (6 December 2004), Sub-Section on "Secrecy Legislation", para. 3; *Report on the Protection of Sources and Whistleblowers*, United Nations Special Rapporteur on Freedom of Opinion and Expression, A/70/361, 2017, para. 47; and the *Global Principles on National Security and the Right to Information* (The Tshwane Principles), developed and adopted on 12 June 2013 by a large assembly of experts from international organisations, civil society, academia and national security practitioners, Principle 3(b).

terrorism, separatism and incitement to breach military discipline."[7] 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),[8] can serve as useful guidance when developing a framework for the handling of classified information.[9]

14. As set out in Principle 6 of Tshwane Principles, "*all oversight, ombuds, and appeal bodies, including courts and tribunals, should have access to all information, including national security information, regardless of classification level, relevant to their ability to discharge their responsibilities*". The access to classified information may be fundamental for judges and prosecutors to effectively carry out their duties, ensuring that justice is served and legal processes with all relevant safeguards are upheld. This access is crucial for informed decision-making, upholding the rule of law, protecting the rights of individuals involved in judicial proceedings and ensuring the equality of arms during such proceedings. By having access to relevant classified information, judges and prosecutors can better assess cases, guarantee fair trial rights, and maintain the integrity of the justice system. It also allows the judiciary to be an accountability mechanism for the security sector. At the same time, the state has also an interest in ensuring the protection of classified information and may develop procedures or mechanisms for that purpose, such as some form of security clearance. However, any such procedures or mechanisms shall not infringe upon judicial and prosecutorial independence.

1. THE RIGHT TO A FAIR AND PUBLIC HEARING BY AN INDEPENDENT AND IMPARTIAL TRIBUNAL

15. The independence of the judiciary is a fundamental principle and an essential element of any democratic state based on the rule of law.[10] The principle is also crucial to upholding other international human rights standards.[11] This independence means that both the judiciary as an institution and individual judges must be able to exercise their professional responsibilities without being influenced by the executive or legislative branches or other external sources.[12]

16. At the international level, it has long been recognized that litigants in both criminal and civil matters have the right to a fair hearing before an "*independent and impartial tribunal*", as guaranteed by Article 14 of the International Covenant on Civil and Political Rights

7 ECtHR, *National security and European case-law*, 2013, para. 5.

8 See Parliamentary Assembly of the Council of Europe (PACE), *Resolution 2060 on Improving the Protection of Whistleblowers* (2015), endorsing the 2013 *Global Principles on National Security and the Right to Information* (The Tshwane Principles).

9 *Ibid.* Principle 9 (2013 Tshwane Principles).

10 See UN Human Rights Council, Resolution on the Independence and Impartiality of the Judiciary, Jurors and Assessors, and the Independence of Lawyers, *A/HRC/29/L.11*, 30 June 2015, which stresses "*the importance of ensuring accountability, transparency and integrity in the judiciary as an essential element of judicial independence and a concept inherent to the rule of law, when it is implemented in line with the Basic Principles on the Independence of the Judiciary and other relevant human rights norms, principles and standards*". As stated in the *1990 OSCE Copenhagen Document*, "*the rule of law does not mean merely a formal legality which assures regularity and consistency in the achievement and enforcement of democratic order, but justice based on the recognition and full acceptance of the supreme value of the human personality and guaranteed by institutions providing a framework for its fullest expression*" (para. 2).

11 See *OSCE Ministerial Council Decision No. 12/05* on Upholding Human Rights and the Rule of Law in Criminal Justice Systems, 6 December 2005.

12 See e.g., UN Human Rights Committee, *General Comment No. 32 on Article 14 of the ICCPR*, para. 19; see also the overview of the caselaw of the European Court of Human Rights relating to Article 6 (1) of the ECHR in *Guide on Article 6 of the ECHR – Right to a Fair Trial (civil limb)* (August 2023) (in particular ECtHR, *Ástráðsson v. Iceland* [GC], no. 26374/18, 1 December 2020, paras. 207 and seq.). See also Venice Commission, *Rule of Law Checklist*, 2016, para. 74.

(ICCPR),[13] Article 6 of the European Convention for the Protection of Human Rights and Fundamental Freedoms[14] (ECHR) and Article 47 of the EU Charter of Fundamental Rights. OSCE participating States have also committed to ensuring that the independence of the judiciary is guaranteed in law and respected in practice, recognizing the independence of judges and the impartial operation of the public judicial service as elements of justice that are essential to the full expression of the inherent dignity and equal and inalienable rights of all human beings.[15]

17. International understanding of the practical requirements of judicial independence continues to be shaped by the work of international mechanisms, including the UN Human Rights Committee, the caselaw of the European Court of Human Rights (ECtHR)[16] and of the Court of Justice of the European Union (CJEU),[17] as well as the development of soft-law instruments and other non-legally binding guidance documents.[18] Article 14 of the ICCPR and Article 6 of the ECHR refer to "national security" as a possible ground to exclude the press and public from all or part of a trial but not to justify other restrictions to the fair trial and due process guarantees provided under these provisions. The Siracusa Principles on the Limitation and Derogation Provisions in the ICCPR and the UN Human Rights Committee's General Comment explain that the denial of certain fair trial rights can never occur, even in an emergency situation, because "*the principles of legality and the rule of law require that fundamental requirements of fair trial [including to be tried by an independent and impartial tribunal] must be respected during a state of emergency*"; in addition, *"national security cannot be used as a pretext for imposing vague or arbitrary limitations and may only be invoked when there exist adequate safeguards and effective remedies against abuse*".[19]

---

13 UN International Covenant on Civil and Political Rights (hereinafter "ICCPR"), adopted by the UN General Assembly by resolution 2200A (XXI) of 16 December 1966. The Republic of Poland ratified the ICCPR on 18 March 1977. See also UN Human Rights Committee, *General Comment No. 32 on Article 14 of the ICCPR: Right to Equality before Courts and Tribunals and to Fair Trial*, 23 August 2007, which provides guiding interpretation of Article 1 of the ICCPR.

14 The Council of Europe's Convention for the Protection of Human Rights and Fundamental Freedoms (hereinafter "ECHR"), signed on 4 November 1950, entered into force on 3 September 1953. The Republic of Poland ratified the ECHR on 19 January 1993.

15 See *1990 OSCE Copenhagen Document*, paras. 5 and 5.12; *Document of the Moscow Meeting of the Conference on the Human Dimension of the CSCE* (Moscow, 10 September-4 October 1991); *Ministerial Council Decision No. 7/08 on Further Strengthening the Rule of Law in the OSCE Area*, Helsinki, 4-5 December 2008. See also *ODIHR Kyiv Recommendations on Judicial Independence in Eastern Europe, South Caucasus and Central Asia (2010, Kyiv Recommendations)*, developed by a group of independent experts under the leadership of ODIHR and the Max Planck Institute for Comparative Public Law and International Law – Minerva Research Group on Judicial Independence; and the *ODIHR Recommendations on Judicial Independence and Accountability (2023, Warsaw Recommendations)* (2023), which aim to supplement the *ODIHR Kyiv Recommendations* by elaborating on certain, previously unaddressed issues and to respond to developments since 2010; the two documents should be read in tandem. See also ODIHR, *Legal Digest of International Fair Trial Rights* (2012).

16 See the overview of the caselaw of the European Court of Human Rights (ECtHR) relating to Article 6 (1) of the ECHR in *Guide on Article 6 of the ECHR – Right to a Fair Trial (civil limb)* (August 2023) (in particular ECtHR, *Ástráðsson v. Iceland* [GC], no. 26374/18, 1 December 2020, paras. 207 and seq.).

17 See e.g., Court of Justice of the European Union (CJEU), *Criminal proceedings against WB and Others*, Joined Cases C-748/19 to C-754/19, 16 November 2021, para. 67; W.Ż., C-487/19, preliminary ruling request by the Supreme Court (Civil Chamber) of Poland (regarding the Chamber of Extraordinary Control and Public Affairs of the Supreme Court), 6 October 2021, para. 109; *Commission v. Poland*, C-791/19, 15 July 2021, para. 59; *A.B.* [GC], C-824/18, 2 March 2021, para.117; CJEU, *A. K. and Others v. Sąd Najwyższy, CP v. Sąd Najwyższy and DO v. Sąd NajwyższyA. K. and Others v. Sąd Najwyższy, CP v. Sąd Najwyższy and DO v. Sąd Najwyższy* [GC], C-585/18, C-624/18 and C-625/18, 19 November 2019, paras. 121 and 122; *Commission v. Poland* [GC], C-619/18, 24 June 2019, paras. 73 and 74; *Associação Sindical dos Juízes Portugueses*, C-64/16, 27 February 2018, para. 44.

18 See e.g., UN Human Rights Committee, *General Comment No. 32 on Article 14 of the ICCPR*; see also *UN Basic Principles on the Independence of the Judiciary*, endorsed by UN General Assembly resolutions 40/32 of 29 November 1985 and 40/146 of 13 December 1985; and *Bangalore Principles of Judicial Conduct*, endorsed by the UN Economic and Social Council in its resolution 2006/23 of 27 July 2006; and *Measures for the Effective Implementation of the Bangalore Principles of Judicial Conduct* (2010), prepared by the Judicial Group on Strengthening Judicial Integrity. See also *ODIHR Kyiv Recommendations on Judicial Independence in Eastern Europe, South Caucasus and Central Asia (2010, Kyiv Recommendations)*, and the *ODIHR Recommendations on Judicial Independence and Accountability (2023, Warsaw Recommendations)* (2023).

19 See UN ECOSOC, Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights, UN Doc E/CN.4/1985/4, Annex (1985), para. 70(g). See also UN Human Rights Committee, CCPR General Comment 29 (2001), para. 16.

18. Where judges or prosecutors are called upon to access confidential information in the course of the exercise of their duties, several fair trial guarantees may come into play. These include the right to be tried by an independent and impartial tribunal, if the access to classified information implies some form of control or oversight by the intelligence/security service. Security clearance of judges, especially when carried out by an executive body or security agency, such as an intelligence or security service, may potentially lead to an external influence or pressure. The right to equality of arms may also be unduly impacted when a party to a trial is prevented from accessing certain information because they are classified for national security purpose or where judicial control by a court is limited by national security reasons.

2. THE AUTONOMY AND INDEPENDENCE OF THE PROSECUTION SERVICE

19. A series of international documents sets a framework of standards and recommendations related to the work, status and role of the prosecution service. These instruments include the 1990 UN Guidelines on the Role of Prosecutors, which aim to assist UN Member States in securing and promoting the effectiveness, impartiality and fairness of prosecutors in criminal proceedings.[20] Other important principles are contained in the 1999 International Association of Prosecutors' Standards of Professional Responsibility and Statement of the Essential Duties and Rights of Prosecutors.[21] Further standards are outlined in the UN Convention against Corruption (UNCAC), which calls upon States Parties to take measures to strengthen the integrity of the prosecution services and prevent opportunities for their corruption, bearing in mind their crucial role in combating corruption.[22]

20. The Council of Europe's Committee of Ministers also formulated fundamental principles concerning the role of the public prosecution service.[23] The Rome Charter, adopted by the Consultative Council of European Prosecutors (CCPE) in 2014, proclaims the principle of independence and autonomy of prosecutors, and the CCPE recommends that the *"[i]ndependence of prosecutors […] be guaranteed by law, at the highest possible level, in a manner similar to that of judges".*[24] Certain principles related to the prosecution service are also contained in OSCE commitments, such as the 1990 Copenhagen Document, which provides that "*the rules relating to criminal procedure will contain a clear definition of powers in relation to prosecution and the measures proceeding and accompanying prosecution*".[25] Lastly, the 2006 Brussels Declaration on Criminal Justice Systems states that "*[p]rosecutors should be individuals of integrity and ability, with appropriate training and qualifications; prosecutors should at all times maintain the honour and dignity of their*

20 The *1990 UN Guidelines on the Role of Prosecutors* were adopted by the 8th UN Congress on the Prevention of Crime and the Treatment of Offenders, Havana, Cuba, 27 August to 7 September 1990.

21 See *International Association of Prosecutors, Standards of Professional Responsibility and Statement of the Essential Duties and Rights of Prosecutors*, approved by the International Association of Prosecutors on 23 April 1999. These Standards were annexed to resolution 2008/5 of the Commission on Crime Prevention and Criminal Justice of the UN Economic and Social Council on "Strengthening the rule of law through improved integrity and capacity of prosecution services", which also requested States to take these Standards into consideration when reviewing or developing their own prosecution standards.

22 See Article 11 of the *UNCAC*.

23 See *Recommendation Rec(2000)19 of the Committee of Ministers to Member States* on the Role of Public Prosecution in the Criminal Justice System (6 October 2000); and *Recommendation CM/Rec(2012)11 of the Committee of Ministers* to Member States on the Role of Public Prosecutors outside the Criminal Justice System (19 September 2012). See also Parliamentary Assembly of the Council of *Europe, Recommendation 1604 (2003) on the Role of the Public Prosecutor's Office in a Democratic Society Governed by the Rule of Law* (27 May 2003).

24 See Consultative Council of European Prosecutors (CCPE), *Rome Charter – Opinion no. 9 (2014) on European Norms and Principles concerning Prosecutors*, para. 33.

25 See *OSCE Copenhagen Document 1990*, para. 5.14.

profession and respect the rule of law" and that *"[t]he office of prosecutor should be strictly separated from judicial functions, and prosecutors should respect the independence and the impartiality of judges"*.[26]

3. THE RIGHT TO RESPECT FOR PRIVATE AND FAMILY LIFE

21. Security clearance mechanisms also involve an interference with the right to respect for private and family life which is protected *inter alia* by Article 17 of the ICCPR, Article 8 of the ECHR and Article 7 of the EU Charter of Fundamental Rights. According to the case-law of the ECtHR, the collection and storage of personal information by a government agency, as well as the transfer of data records between agencies, fall within the ambit of Article 8 of the ECHR.[27] Interference with the right to private life is only acceptable if it is covered by the limitations contained in Article 8 (2) of the ECHR and if it is proportionate to the aim pursued, including the protection of national security.

V. APPLICATION OF STANDARDS AND GOOD PRACTICE

1. GENERAL CONSIDERATIONS

22. As noted above, security clearance of judges, especially when carried out by an executive body or security agency, such as an intelligence or security service, may potentially result in, or be perceived as, exercise of external influence or pressure by the executive over the judiciary and prosecution service, potentially jeopardizing their independence. Indeed, a situation where the executive is able to control, direct or influence the judiciary is incompatible with the notion of an independent tribunal.[28]

23. Several soft law instruments, opinions or reports of international or regional human rights bodies and caselaw of international courts underline the inherent risks for judicial independence when having some form of security clearance of judges or prosecutors carried out by an executive body.

24. In its caselaw, the ECtHR analyzed the mechanism of security clearance by the National Security Agency of judges of the (now abolished) Special Court in Slovakia, which was in charge of adjudicating cases of corruption, organized crime and other serious offences committed by high level officials. At the outset, the Court underlined that the key issue related to the independence of the judge's status, in particular with regard to the requirement for security vetting clearance which was issued and could be withdrawn by the National Security Agency, an executive body. Though noting that such judges are career judges whose term of office was not limited in time, it underlined that they could nevertheless be recalled from the Special Court if they ceased to meet the security vetting criteria, hence potentially impacting the irremovability of judges by the executive during their term of office. This

26 See the *2006 Brussels Declaration on Criminal Justice Systems*, 5 December 2006.
27 See e.g., ECtHR, *Amann v. Switzerland* [GC], no. 27798/95, 16 February 2000; European Commission of Human Rights, *Chave née Jullien v. France (dec.)*, no. 14461/88, 9 July 1991.
28 See UN Human Rights Committee, *General Comment No. 32 on Article 14 of the ICCPR*, para. 19.

principle is a corollary of judicial independence, which is among the key guarantees of Article 6 (1) of the ECHR.[29] Looking at how such provisions were implemented in practice, the Court observed that there was no indication of any specific instance of withdrawal of a judge's security vetting certificate, noting the possibility to challenge the withdrawal before a special parliamentary committee and, ultimately, before the Supreme Court and the Constitutional Court. The Court concluded that in light of the procedure, there were no grounds for the applicant to have legitimate misgivings as to the "independence" of the Special Court, which tried the applicant, and the Special Division of the Supreme Court which determined the appeal.

25. When reviewing a mechanism whereby security checks of serving judges was contemplated, to be carried out by the Security Intelligence Agency of Croatia (i.e., an executive body) as part of the integrity check of judges, the Venice Commission stressed in its Opinion that the necessity for such a far-reaching reform must be well substantiated, noting the already existing wide array of mechanisms to ensure integrity of the judicial corpus.[30] The Venice Commission also noted the risk that the application of such a mechanism by an executive body would have in terms of aggravating the public perception of alleged interference or pressure from government and politicians on the judiciary, ultimately further impacting the public trust in the judiciary.[31] The Venice Commission therefore recommended that the Croatian authorities reconsider the introduction of periodic security vetting of all serving judges and that they develop an alternative strategy to ensure judges' integrity, based on other existing mechanisms.

26. The *ODIHR Kyiv Recommendations on Judicial Independence in Eastern Europe, South Caucasus and Central Asia (2010 Kyiv Recommendations)*, underline that, during judicial selection/appointment processes, beyond standard check for a criminal record and any other disqualifying grounds from the police, no other background checks should be performed by any security services.[32]

2. EXAMPLES OF STATE PRACTICES

27. At the outset, it is important to emphasize that due to differing institutional frameworks and histories, domestic legal systems may have developed diverse types of checks and balances between the different branches of powers. However, all such frameworks shall meet international standards. In this respect, it is important to balance national security interests and respect for judicial and prosecutorial independence. Even where national security is at stake, the fundamental principles of fair trial, including respect for judicial independence, should be respected.

29 See ECtHR, *Fruni v. Slovakia*, no. 8014/07, 21 June 2011, paras. 143-145.
30 See Venice Commission, *Opinion on the introduction of the procedure of renewal of security vetting through amendments to the Courts Act in Croatia*, CDL-AD(2022)005-e, paras. 16-17.
31 *Ibid.* para. 18.
32 See 2010 *ODIHR Kyiv Recommendations*, para. 22.

28. From a non-exhaustive overview of state practices relating to judges/prosecutors' access to classified information, there tends to be three main models, although the first one appears to be prevailing:

    a. *Ex officio* access to classified information by all (or part) of judges and prosecutors without any form of security clearance;[33]

    b. Special security clearance mechanism for judges or prosecutors handling cases involving classified information,[34] for instance when a special court or chamber deals with organized crime, terrorism or other similar criminal offences and/or need to access and handle sensitive materials in possession of intelligence or security agencies;

    c. No access to classified information by default, with the competent security or intelligence body de-classifying the relevant information for the purpose of judicial proceedings or other circumstances.[35]

29. With respect to the first category, in the majority of countries, the legislation on protection of classified information or state secrets exempts all judges and prosecutors, or at least certain categories of high-level judges and prosecutors, from verification proceedings to get security clearance.[36] Hence, judges and prosecutors do not require verification or specific security clearance, before being entitled to access classified information. In general, national security agencies do not conduct security checks on candidate judges or existing judges,[37] although some forms of checks of police records are carried out for candidate judges before appointment. At times, states may choose to differentiate judges' access to categories of

33 See e.g., in **Bosnia and Herzegovina,** the Law on Protection of Secret Data provides that judges and prosecutors do not need security clearance to access secret data ; **Bulgaria** (Classified Information Protection Act, Article 39 (1)); **Serbia,** Article 38 of the Data Secrecy Law provides that judges shall be authorized to access data of all levels of classification that they need in order to perform tasks in their purview, without security clearance including info marked "TOP SECRET" and "SECRET"; **Lithuania,** the Law on State Secrets and Official Secrets provides that judges shall, in exercising their powers, have the right to familiarise with classified information and to use it; in **Slovenia,** judges and prosecutors can access classified information without needing a security clearance (see Article 3 of the *Classified Information Act of Slovenia*, Official Gazette of RS, No. 50/06); the **United States of America**, the so-called Article III judges, who are nominated by the President and confirmed by the US Senate, are automatically entitled to access to classified information necessary to resolve issues before them, but their law clerks must obtain security clearances to have access to classified information

34 See e.g., in **Hungary**: all regional court presidents, vice presidents and judges who permit intelligence data gathering or deal with cases related to classified information need to undergo a security check by the National Security Agency, before assuming their responsibilities and then every five years (Section 71/C, paragraph (7), of Act CXXV of 1995 on National Security and Sections 42/A to 42/C of Act CLXII of 2011 on the Status and Remuneration of Judges); **Norway**, a security clearance process is required only for judges who want to hear national security cases (see Section 21 of the Act relating to the Courts of Justice Act, which provides that "*only judges who have the necessary clearance and are authorised for the security level concerned shall participate*"). In **England and Wales**, when Crown Prosecutors need to access sensitive material generated by, or in possession of, the security and intelligence agencies that is potentially relevant to an investigation, security clearance is required; see *Disclosure Manual*: Chapter 33 - Access to and Handling Highly Sensitive Third-Party Material, 21 October 2021.

35 In **France** and **Italy**, judicial authorities can only access declassified or open materials, while "secret information" cannot be used in court; see *European Parliament Study*: National Security and Secret Evidence in Legislation and before the Courts (2014).

36 See e.g., in **Bulgaria** (the general rule under section 36 of the Protection of Classified Information Act 2002 is that no official can access classified information unless holding the appropriate level of security clearance, although the holders of a number of posts, including constitutional judges, judges and prosecutors) are, however, not subjected to such vetting and obtain a security clearance allowing them access to all levels of classified information (subject, however, to the "need to know" principle); **Slovenia,** judges and prosecutors can access classified information without needing a security clearance (see Article 3 of the *Classified Information Act of Slovenia*, Official Gazette of RS, No. 50/06). In **Latvia**, only judges of the courts which are lower in the court hierarchy have to undergo a special procedure (see p. 44 <https://www.aca-europe.eu/images/media_kit/seminars/2017_Cracow/2017_KRK_GeneralReport.pdf>).

37 See e.g., within the European Union, the national security agency does not carry out security checks on judges or candidate judges in **Belgium**, **Bulgaria**, **Ireland**, **Greece**, **Spain**, **France**, **Poland**, **Malta**, **Cyprus**, **Luxembourg**, **Netherlands**, **Austria**, **Romania**, **Slovenia**, **Slovakia**, **Finland**, **Sweden** (and **Croatia**, since the provisions were annulled by the Constitutional Court on 7 February 2023). In some countries, security checks are carried out by the national security agency for *candidate judges* before appointment, either upon an explicit request (**Germany**, **Czech Republic**, **Italy** and **Portugal**) or systematically (**Denmark**, **Estonia**, **Latvia** and **Lithuania**).

information based on the level of secrecy and have special mechanism in place when accessing the highest level of classified information (e.g., highest secrecy level).[38]

30. In several countries, there have been recent legislative initiatives, or attempts, to introduce some form of security checks of judges and prosecutors by an executive body or security service, although not necessarily for the purpose of granting them access to classified information, some of which have been met with strong criticisms or even been held unconstitutional as unduly impacting judicial independence.[39]

3. General Guiding Principles and Recommendations

31. As underlined above, access to classified information may be necessary for the fulfillment of the duties of judges and prosecutors.[40] When carrying out their functions, judges and prosecutors may be required to have access to classified materials to effectively assess the substance of the case, to make informed decisions, uphold the rule of law, and protect the rights of individuals involved in the justice system.

32. Ensuring accountability, transparency and integrity are essential elements of judicial independence and a concept inherent to the rule of law, when implemented in line with human rights norms, principles and standards. In order to comply with the requirements of judicial and prosecutorial independence and principle of separation of powers, the judges and prosecutors concerned must be and be perceived to be independent of the executive and the legislature at all stages of the proceedings[41] and when carrying out their functions.

33. In light of the principles stated above, and state practices, **the introduction of any mechanism of security clearance carried out by a national security service or another executive body should be discouraged in light of its potential to infringe upon judicial and prosecutorial independence**. In case of security breaches or mishandling of classified information by judges or prosecutors, with respect to judges and prosecutors handling classified information, the use of existing disciplinary and/or criminal procedures and

38 For instance, in **Sweden**, the Judicial Appointments Board, an independent judicial body, conducts the verification procedure for all security levels for *court presidents*, based on a questionnaire and each court performs the verification procedure for all security levels for first or second instance judges, with the Swedish Security Service conducting a records check (whether the candidate has been referred to in its records in any way, but does not collect information) only before a person may take part in security sensitive activities; for court presidents, the government decides which positions are to be classified for security on the highest security level and the Government Office decides which positions are to be classified for security on the lower security levels; for first or second instance judges, the government decides which positions are to be classified for security on the highest security level and the court decides which positions are to be classified for security on the lower security level.

39 See e.g., in **Belgium** (attempt of the government – now withdrawn – to introduce initial and regular (every five years) security checks on all judges, heavily criticized by the High Council of Justice noting the threat to the separation of powers due to the risk of interference by the executive in the functioning of the judiciary; see *2023 Rule of Law Report - Country Chapter on the rule of law situation in Belgium*, 5 July 2023, p. 5; and *2024 Rule of Law Report*, p. 5; **Croatia** (periodic security checks conducted by the National Security Agency on all judges and state attorneys were introduced in 2022 but were annulled by the Constitutional Court on 7 February 2023, U-I-2215/2022, as being unconstitutional, see *2023 Rule of Law Report - Country Chapter on the rule of law situation in Croatia*, July 2023; see also Venice Commission, *Opinion on the introduction of the procedure of renewal of security vetting through amendments to the Courts Act in Croatia*, CDL-AD(2022)005-e); **Slovakia**, where the Slovak Constitutional Court, in a landmark ruling, PL. ÚS 21/2014, on 30 January 2019, held that the background checks on judges and candidate judges on the basis of information from the Slovak National Security Authority were in breach of the principle of judicial independence and that the constitutional amendment dating from 2014 was unconstitutional.

40 According to Principle 6 of the *Tshwane Principles*, all oversight and appeal bodies, including courts and tribunals, should have access to all information, including national security information, regardless of classification level, relevant to their ability to discharge their responsibilities.

41 See ODIHR *Urgent Interim Opinion on the Bill amending the Act on the Organization of Common Courts, the Act on the Supreme Court and Certain Other Acts of Poland* (as of 20 December 2019), para. 38, 14 January 2020.

sanctions, proportionate to the gravity of the offence, should be used, provided these are effective mechanisms.

34. However, should the legal drafters demonstrate the necessity to introduce a mechanism of security clearance for judges and prosecutors, this should be accompanied by adequate safeguards avoiding the risk of perceived or actual undue political influence or pressure over the judiciary and prosecution services. Careful consideration must be given to clearly and precisely defining the personal scope of such clearance - on an *ad hoc* basis as required for the exercise of their functions or duties, as well as the nature and modalities and institutional framework, to avoid a risk of arbitrary application by the public authorities and ensure there is no undue infringement upon judicial and prosecutorial independence during the security clearance process. The requirements and procedure should be clearly stipulated in publicly accessible laws, duly justified, strictly necessary and proportionate to the objective of verification (see further Sub-Section 3.3. below).

3.1. Personal Scope of the Security Clearance Process

35. As a mechanism of security clearance would likely involve the processing or collection of a wide range of personal data, it would fall within the ambit of Article 8 of the ECHR and Article 17 of the ICCPR. While "national security" constitutes one of the legitimate aims that may justify restrictions to the right to respect for private and family life, the authorities should demonstrate that the contemplated measures are necessary and proportionate in relation to the aim pursued. It is unlikely that authorities may be able to convincingly demonstrate the necessity to run security checks on *all* judges and prosecutors, meaning even those not involved in any way in security, terrorism, organized crime or other cases involving the review and handling of classified information. Furthermore, it would also reduce the risk of undue impact on judicial and prosecutorial independence if security clearance process is carried out only with respect to **those judges and prosecutors who are willing or would likely need to access and handle classified information when exercising their judicial or prosecutorial functions or duties**. Additionally, in order to further narrow down the scope of verification, clearance may only be required for accessing and handling the highest levels of classification (top-secret and secret).

3.2. Competent, Independent and Impartial Body

36. One consideration of utmost importance is to respect the principles of separation of powers and checks and balances, and judicial and prosecutorial independence. If the process is conducted or controlled by the executive, or with the involvement of the executive, it may be (or perceived to be) influenced by the executive. Hence, **one of the key safeguards would be to have an independent, competent, and impartial body in charge of and directly carrying out the security clearance process, such as a judicial or prosecutorial self-governing body or other independent entity,[42] rather than an executive body or security agency, such as the intelligence or security service. The information collected by this (independent) body must be limited, both in law and in practice, to the extent that is strictly necessary for the purpose of the security clearance process.** It would also be recommended **to regulate in detail in the law the key substantive and procedural**

42 E.g., a judicial body (for instance, a special panel composed of Supreme Court judges) deciding on the existence of security obstacles or a judicial council or specific commission within the judicial council. See, as a comparison, with respect to "vetting" of judges, ECtHR, *Xhoxhaj v. Albania*, no. 15227/19, 9 February 2021, paras. 289-294.

safeguards to ensure its independence, namely the composition and appointment procedures of the members of the body, the duration of the mandate of the members, the powers of that body, guarantees of fair trial, the decision-making rules and procedures for appeal, and the question how the members themselves would be vetted.[43] **Even if an executive body or security service contributes to the security clearance process carried out by another (independent) body, its role in the process, both in law and in practice, must be clearly and precisely stipulated in law and limited to the extent strictly necessary for the purpose of the security clearance process**.[44] For example, its involvement should be minimal, e.g., only checking its own records to ensure that the applicant is not referred to therein, but not triggering the direct collection, storage and processing of a larger amount of personal data irrelevant to the purpose of security clearance.[45] If the national security service is involved in carrying out the security clearance, it is recommended that **the final decision on whether or not a judge is issued security clearance should not vest with the security service**.[46]

37. It is also important that the results of the security clearance process be communicated to the concerned person, safe for duly justified security reasons preventing the communication of certain pieces of information, and in conformity with fair trial requirements.[47]

38. Effective internal control and external oversight over the intelligence or security service involved in the security clearance process should also be in place, including of the data banks it maintains, to ensure due respect for judicial and prosecutorial independence and compliance with international human rights standards more generally (see Sub-Section V.5 below).[48]

3.3. Nature and Modalities of the Security Clearance Checks

39. When opting for a system of security clearance for certain judges and/or prosecutors, by which they would be subjected to a verification process prior to accessing classified information, or certain "top secret" information, the nature and modalities of the security checks should include safeguards and ensure due process to respect judicial and prosecutorial independence. In particular, the requirements and procedure for such clearance and possible oversight should be reasonable,[49] and **the conditions and modalities of the security clearance should be clearly and precisely defined in law to avoid a risk of arbitrary application by the public authorities, especially by the body in charge of security clearance. The requirements and procedure should also be duly justified and strictly necessary. In this respect, legislation should not be disproportionate and duplicative of**

43 See e.g., Venice Commission, *Opinion on the introduction of the procedure of renewal of security vetting through amendments to the Courts Act in Croatia*, CDL-AD(2022)005-e, para. 25.

44 See e.g., Venice Commission, *Opinion on the introduction of the procedure of renewal of security vetting through amendments to the Courts Act in Croatia*, CDL-AD(2022)005-e, para. 22.

45 For instance, in **Sweden**, when a judge is willing or needs to access sensitive/classified information, the Swedish Security Service only conducts a records check (whether the candidate has been referred to in its records in any way) but does not collect information, which is done via questionnaire by the Judicial Appointment Board for court presidents or by the courts themselves for first and second instance judges.

46 As a comparison, with respect to the security clearance of certain parliamentarians, in **Estonia**, the respective security/intelligence agency carries out necessary vetting procedures but final decision rests with the Parliament, see <https://www.nato-pa.int/download-file?filename=/sites/default/files/2019-06/DCAF%20NATO%20PA_%20Survey_Report_Revised%20NYS2611_FINAL%20%28002%29.pdf>, pp. 26-27.

47 See e.g., Venice Commission, *Opinion on the introduction of the procedure of renewal of security vetting through amendments to the Courts Act in Croatia*, CDL-AD(2022)005-e, para. 23.

48 *Ibid.* para. 24.

49 See e.g., Principle 32 (a) of the *Tshwane Principles*.

existing measures aimed at ensuring judicial integrity, such as asset declarations or disciplinary proceedings, and should provide robust oversight and accountability framework.[50]

40. Since a security clearance process is likely to involve some inquiries pertaining to the private and family life of an individual judge or prosecutor, it is fundamental that the nature and modalities of the security clearance checks comply with the right to respect for private and family life. In particular, only the information that would be adequate and relevant for the purpose of the security clearance should be processed, and special categories of sensitive data, for instance pertaining to health status,[51] should in principle not be processed. Moreover, the level of details to be provided, for instance with respect to movable property or assets which generally may not be recorded, should not create an undue burden on them.[52] Also, the information provided by judges and prosecutors during the security clearance process should not be used as evidence in criminal proceedings, or this may otherwise be considered contrary to the right to remain silent and not to incriminate oneself, protected under Article 6 (2) of the ECHR and Article 14 (2) of the ICCPR.[53]

41. The assessment criteria for concluding on the existence of security risk preventing the granting of security clearance, should be specified clearly in the law. In addition, the law should provide for an explicit presumption in favour of the judge subject to security clearance: if the information is not sufficient to clearly establish a security risk, there should not be any consequences for him or her as a result of the security clearance process.[54]

3.4. Effective Remedy

42. The principle of irremovability of judges who are security-cleared, as a corollary of their independence, should be guaranteed. This means that **the body in charge of security clearance should not have the power to unilaterally decide the withdrawal of the security clearance for allegations of no longer meeting the security clearance criteria, without proper justification and due process guarantees for the said judge, including the possibility to challenge the withdrawal before an independent and impartial tribunal**.[55]

43. More generally, **the judges and prosecutors subject to security clearance should have access to an effective remedy to challenge the refusal to grant or the withdrawal of security clearance**, particularly when it affects the judge's 'civil rights' in the sense of Article 6 of the ECHR. The more serious the consequences, the more important are such rights of effective review. The subject of security clearance should be provided with the reasons for such a withdrawal or refusal to grant the clearance. Where, in the course of the clearance process, the judge or prosecutor was required to provide information, and if subsequently this information is used to subject this judge or prosecutor to criminal proceedings, it is important to assess whether this is compatible with the right to remain silent and not to incriminate oneself, contained in Article 6 (2) of the ECHR.

50 See Venice Commission *Report* on the Independence of the Judicial System Part I, 16 March 2010.
51 See Council of Europe Convention 108 + for the protection of individuals with regard to the processing of personal data, Article 6, ratified by Poland on June 2020 (not yet in force, awaiting 38th ratification).
52 See e.g., Venice Commission, *Opinion on the introduction of the procedure of renewal of security vetting through amendments to the Courts Act in Croatia*, CDL-AD(2022)005-e, para. 29.
53 *Ibid.* para. 30.
54 *Ibid.* para. 33.
55 See e.g., ECtHR, *Fruni v. Slovakia*, no. 8014/07, 21 June 2011, paras. 143-145.

3.5. Confidentiality of Any Information Collected and Compliance with Personal Data Protection Standards

44. Given the sensitivity of the information that may be collected during the security clearance process, it is fundamental that their confidentiality be guaranteed and that full compliance with international personal data protection standards be ensured. As per international standards, publicly available law should outline the types of personal data that security services may hold, and which criteria apply to the use, retention, deletion and disclosure of these data. In this respect the use of personal data should be strictly limited and confined to its original specified purpose; necessary measures should be taken to ensure that records of personal data are accurate; personal data files should be deleted when no longer required; and individuals have the right to have access to and correct their personal data file. [56]

3.6 Liability for Mishandling Classified Information by Security-Cleared Judges and Prosecutors

45. With the granting of security clearance comes significant responsibility. Those judges and prosecutors who have been security-cleared must exercise caution in handling and sharing classified information. They must ensure that such information is not disclosed in a manner that could compromise national security, endanger individuals, or disrupt public order.[57]

46. The Tshwane Principles provide that any public personnel who believe that information has been improperly classified should be able to challenge such classification (Principle 14). They also offer useful guidance with respect to the disclosure by public personnel of information, regardless of its classification, which shows serious wrongdoing that has occurred, is occurring, or is likely to occur, such as criminal offenses, human rights violations, international humanitarian law violations, corruption, dangers to the environment, among others (Principle 37). In such cases, the public personnel should in principle be protected against retaliation and should enjoy immunity from civil and criminal liability when publicly disclosing serious wrongdoing in the public interest, if the listed conditions are met; whistle-blowers in the public sector should not face retaliation if the public interest in the information disclosed outweighs the public interest in secrecy, though they should have first made a reasonable effort to address the issue through official complaint mechanisms, provided that an effective mechanism exists. (Principles 38-41, and 43). Such principles should *a priori* apply to security-cleared judges and prosecutors.

47. In addition, international standards provide that judges should enjoy immunity for decisions taken or activities carried out in good faith in the exercise of judicial functions (functional immunity).[58] However, like other persons, judges may be subject to civil or criminal

56 Compilation of Good Practices for Intelligence Agencies and their Oversight, Report to the UN Human Rights Council by the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, A/HRC/14/46, Practice 23.

57 See e.g. UN Human Rights Council, 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 A/HRC/14/46 (2011), Practice 8 stating that "Oversight institutions take all necessary measures to protect classified information and personal data to which they have access during the course of their work. Penalties are provided for the breach of these requirements by members of oversight institutions.' And the Tshwane Principles also state that "…the law should require independent oversight bodies to implement all necessary measures to protect information in their possession. (Principle 35 a).

58 See e.g., ECtHR, *Ernst v. Belgium*, no. 33400/96, 15 October 2003, para. 85, holding that barring suit against judges to ensure their independence met the requirement for a reasonable relationship of proportionality between the means used and the aim pursued. See also ODIHR-Venice Commission, *Joint Opinion on the draft amendments to the legal framework on the disciplinary responsibility of judges in the Kyrgyz Republic* (CDL-AD(2014)018), para. 37. See also UN Special Rapporteur on the independence of judges and lawyers, *Report on*

responsibility for breaches of civil or criminal legislation committed outside their judicial office. At the same time, the disclosure of classified information should only lead to criminal liability in limited cases involving highly sensitive categories of information (such as technological data about nuclear weapons; intelligence sources, codes and methods; diplomatic codes; identities of covert agents; and intellectual property in which the government has an ownership interest and knowledge of which could harm national security), and where the disclosure of such information would pose a real and identifiable risk of causing significant harm. Any sanctions should be proportionate and the proceedings should allow for the possibility to raise a public interest defence.[59]

48. Hence, when not falling within the scope of the above exceptions, should security-cleared judges and prosecutors be investigated for allegations of criminal offences for breaches of national security, for instance for disclosure of state secrets or classified information, standard disciplinary procedures and criminal procedure rules should apply. The Warsaw Recommendations have clarified that "*judges who commit a criminal offence in the exercise of their office should not have immunity from criminal prosecution*."[60] Judges, like all citizens, are subject to the law. If they violate national security legislation, they should face criminal prosecution separately from any disciplinary actions, in accordance with the principles of the rule of law and equality before the law. However, appropriate procedural safeguards should be put in place to protect judges from vexatious or manifestly ill-founded complaints that have the sole aim of threatening or putting pressure on them. In some jurisdictions, the procedure aimed at lifting judicial immunity requires the intervention of a judicial council or a similarly independent authority, while in other countries the authorization to proceed is given by the Head of State or the parliament.[61] As to disciplinary offenses, they must be clearly defined by law, ensuring that any breach of national security falls within these parameters for investigation.

4. MECHANISMS OF INTERNAL CONTROL AND OVERSIGHT OF SECURITY SERVICES TO ENSURE RESPECT FOR JUDICIAL AND PROSECUTORIAL INDEPENDENCE DURING THE SECURITY CLEARANCE PROCESS

49. Should intelligence or security services be involved in the process of providing security clearance to judges or prosecutors, it is important that mechanisms and procedures of internal control and external oversight over their activities are in place[62] to ensure that they operate in compliance with laws and international human rights standards. The external oversight body should have a strong mandate, broad powers (including unhindered access to classified information), and necessary financial and human resources to effectively oversee all aspects of the work of security services, including a systemic examination of human rights compliance of their activities. The said oversight body should also be able to carry out follow-up control of information collection, handling of information, information-sharing

the notion of judicial accountability, A/HRC/26/32, 28 April 2014, para. 52; *Opinion No. 3* of the Consultative Council of European Judges to the attention of the CoE Committee of Ministers on the principles and rules governing judges' professional conduct, in particular ethics, incompatible behaviour and impartiality (2002), para. 52; and Venice Commission, *Amicus Curiae Brief of the Venice Commission on the Immunity of Judges for the Constitutional Court of Moldova*, CDL-AD(2013)008, of 11 March 2013, para. 19.

59 See e.g., Principle 46 b of the *Tshwane Principles*.

60 See *Warsaw Recommendations*, para. 16.

61 See *Report of the Special Rapporteur on the independence of judges and lawyers*, A/75/172, 17 July 2020, para. 52.

62 See e.g., Venice Commission, *Opinion on the introduction of the procedure of renewal of security vetting through amendments to the Courts Act in Croatia*, CDL-AD(2022)005-e, para. 24.

with other authorities and retention/deletion measures, including when they concern judges and prosecutors in the context of the security clearance process. It could also be in charge of receiving complaints from judges or prosecutors against security/intelligence services alleging undue infringements of their independence and/or cases of discrimination or other human rights violations, unless an effective and efficient complaints mechanism already exists for that purpose. The applicable legislation should stipulate who can apply to challenge the legality of the security services' actions or alleged actions, the relevant procedure or court, the grounds for upholding an application and the available remedies. It is also essential to provide for internal complaint channels and whistle-blower protection for members of security services who come across wrongdoing in security clearance/surveillance procedures, including when they concern judges/prosecutors, as an important internal control mechanism.[63] 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.[64]

50. More generally, 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.[65] 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.[66] It is also important that all staff members of security/intelligence services, from senior management to administrative and service staff, are required to participate in training on international human rights law and standards, including judicial independence, as well as practical implementation of professional and ethical codes of conduct in their daily work.[67]

51. It is also essential that proper accountability mechanisms are in place in case of violation of international human rights standards. National laws should 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.[68]

5. RECOMMENDATIONS RELATED TO THE REFORM PROCESS

52. OSCE participating States commit 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*

63 See 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 70.

64 See 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, 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*.

65 CoE Commissioner for Human Rights, *Issue Paper on Democratic and Effective Oversight of National Security Services*, (2015), page 58; 2007 Venice Commission's *Report on the Democratic Oversight of the Security Services),* paras. 15 and 132-133.

66 EU FRA, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU* - Volume II: field perspectives and legal update (Luxembourg, 2017), page 70.

67 As a comparison – for NHRI, see ibid. page 87.

68 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),* Practice 16.

applicability" (1990 Copenhagen Document, paragraph 5.8).[69] Moreover, these 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, para. 18.1).[70] As also provided in the ODIHR Guidelines on Democratic Lawmaking for Better Laws, "*the entire legislative process — whereby policies and laws are designed, drafted, debated, adopted, implemented, monitored and evaluated — should, as a rule, be open and transparent*."[71] The Venice Commission's Rule of Law Checklist also emphasizes that the public should have a meaningful opportunity to provide input.[72]

53. In particular, it is key that policy and legislation relating to national security are developed taking into consideration security needs and concerns that are defined in an inclusive manner,[73] More generally, states should apply a holistic, participatory and transparent approach to security sector reform, based on an inclusive dialogue process among and between authorities at various levels, from all branches of government and security sector institutions, national human rights institutions, civil society,[74] and other non-State actors.[75] When concerning or impacting the judiciary and prosecution service, it is also important to involve their representatives in the public consultation process. This will help increasing local acceptance of security actors, as well as giving them important insights as to how to improve in fulfilling their tasks.[76]

54. Accordingly, policy and legislation regulating the matter of judges and prosecutors' security clearance and access to classified information **should be developed and adopted through a broad, inclusive and participatory process and therefore include the above-mentioned stakeholders in a timely fashion in public discussions to identify policy choices and legislative options**. In particular, an important part of intelligence reform involves actively questioning how intelligence services should be defined in a democratic society and this can only be done through meaningful participation of civil society, academia and media platforms[77] and of all relevant state actors, including the judiciary and prosecution service, especially with respect to the matter under review. 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.[78] To guarantee effective participation, consultation mechanisms should allow for input at an early stage and throughout the process, meaning not only when the draft is being prepared by relevant ministries but also when it is discussed before Parliament.

69 See *1990 OSCE Copenhagen Document*.
70 See *1991 OSCE Moscow Document*.
71 See *ODIHR Guidelines on Democratic Lawmaking for Better Laws*, Principles 6, 7, 8 and 9.
72 See Venice Commission, *Rule of Law Checklist*, Part II.A.5.
73 DCAF – OSCE/ODIHR and UN Women, *Gender and Security Toolkit* (2019), especially *Tool no. 14 on Intelligence and Gender*..
74 OSCE participating States have committed to the aim of "*strengthening modalities for contact and exchanges of views between NGOs and relevant national authorities and governmental institutions*" (Moscow 1991, para. 43.1).
75 UN Secretary-General, *Report on Securing States and Societies: Strengthening the United Nations Comprehensive Support to Security Sector Reform*, 13 August 2013, A/67/970–S/2013/480, para. 61(a).
76 DCAF – OSCE/ODIHR and UN Women, *Gender and Security Toolkit* (2019), Tool no. 1 on Security Sector Governance, Security Sector Reform and Gender, page 27.
77 DCAF – OSCE/ODIHR and UN Women, *Gender and Security Toolkit* (2019), Tool no. 14 on Intelligence and Gender, page 30.
78 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.

55. In light of the above, **the authorities are encouraged to ensure that the ongoing discussions and particularly the reform process is subject to a transparent and inclusive process that involves meaningful and inclusive consultations, including with authorities at various levels, from all branches of government, including the judiciary and prosecution service, and security sector institutions, national human rights institutions, associations, academia, civil society organizations, etc. ODIHR remains at the disposal of the authorities for any further assistance that they may require in any legal reform initiatives on the conditions of access to classified information.**

[END OF TEXT]