

RECOGNISE · RESIST · RISE UP

National Guidelines

for preventing and addressing violence against women in politics
Hungary

Prepared by:

JÓL-LÉT Foundation, the Hungarian implementing partner of the +3R project (Recognise, Resist, Rise Up – against violence against women in politics).

Project lead: Kata Keveházi

Advocacy expert: Dr Bernadett Szél

Legal expert: Dr Andrea Sebestyén



Co-funded by the European Union, CERV 101195093. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the granting authority. Neither the European Union nor the granting authority can be held responsible for them.

Table of Contents

1. Introduction and context.....	4
1.1 Purpose of the guidelines.....	4
The intervention logic of the guidelines	4
How can the guidelines be used?	5
1.2 Political context	5
Why now?	5
1.3 Hungary compared with the +3R partner countries	5
1.4 Key findings of the +3R research and the forms of violence	6
The main forms of violence	6
2. European and international legal framework	6
2.1 The EU Directive on violence against women (2024/1385)	6
2.2 Connection to the Digital Services Act (DSA)	7
2.3 The significance of EU legal harmonisation for violence against women in politics	7
Minimum aspects to examine during transposition	8
2.4 The lack of ratification of the Istanbul Convention	8
2.5 CEDAW: women's political participation and protection against gender-based violence	9
The common message of the European and international framework	9
3. National legal framework	9
3.1 Distinguishing political criticism from gender-based attack.....	10
3.2 Legal protection beyond criminal law	10
4. Police and judicial proceedings	11
4.1 The limits of an incident-based approach	11
4.2 Territorial jurisdiction and effective access to proceedings.....	11
4.3 Risk assessment and safety	12
4.4 Handling digital evidence	12
Recommended procedural minimums	12
5. Institutional capacity and digital protection	12
5.1 Institutional digital-security minimums.....	12
5.2 Rapid response and doxxing.....	13
5.3 Moderation and technical capacity.....	13
5.4 Platform responsibility and the DSA.....	13
6. Training and preparation of the police and the judiciary.....	13
6.1 Minimum content of the training	13
6.2 Not one-off awareness-raising, but professional competence	14
6.3 Protocol and professional support.....	14
6.4 Measuring the impact of training	14
Recommendations	14
7. Political and institutional culture: from recognition to change.....	15
7.1 RECOGNISE - Recognising and naming.....	15
Recognising normalising language.....	15
7.2 RESIST - Resisting normalisation.....	15

7.3 RISE UP - Solidarity, retention and political participation	16
7.4 Regular self-assessment of institutional culture.....	16
Recommendations	16
8. Standards of acceptable conduct	17
8.1 Minimum standard and scope	17
8.2 Consequences and protection against retaliation	17
8.3 Leadership and parliamentary responsibility.....	17
8.4 The Male Pledge and review.....	17
9. Political parties and campaigns	17
9.1 Zero tolerance and leadership responsibility	18
9.2 Mandatory code of conduct.....	18
9.3 Independent and confidential reporting mechanism	18
9.4 Protection against retaliation	18
9.5 Consequences and sanctions	19
9.6 Candidate selection and political advancement.....	19
9.7 Minimum campaign-period protocol	19
9.8 Digital protection and handling of online attacks.....	20
9.9 Support and the person's continued participation in politics	20
9.10 Cross-party solidarity and male allies	20
9.11 Annual institutional self-assessment and monitoring	20
Recommendations	21
10. Institutional support and complaint mechanisms.....	21
10.1 Minimum functions	21
10.2 Independence, confidentiality and conflict of interest	21
10.3 A clear procedure and protection against retaliation.....	21
10.4 Separating support from investigation.....	21
10.5 Monitoring and evaluation	22
10.6 Possible models	22
11. International good practices and their adaptation in Hungary	22
12. Summary recommendations and implementation framework	22
12.1 Short-term priorities.....	22
12.2 Implementation matrix.....	23
12.8 Monitoring and indicators	23
12.9 Annual public status review.....	24
12.10 What does success mean?	24
Glossary	25
A. The phenomenon and its impacts.....	25
B. Institutional and preventive tools	26
C. Legal and policy frameworks	27

1. Introduction and context

1.1 Purpose of the guidelines

This document sets out the national guidelines developed within the Recognise, Resist, Rise Up (+3R) project for preventing, addressing and reducing violence against women in politics (VAWP). It is addressed to all institutions and actors that can play a role in creating the conditions for safe and equal political participation: Parliament and other state institutions, the police and the judiciary, political parties and parliamentary groups, local governments, elected officials and their staff, campaign teams, as well as the media, civil society and other actors shaping public spaces.

For the purposes of these guidelines, "women in politics" does not refer solely to elected officials. The concept extends to candidates, members and officeholders of political parties, parliamentary and local-government staff, political advisers, members of campaign teams, activists, and other women engaged in political or public life.

The guidelines pay particular attention to the fact that the risks and consequences of political violence do not affect all women in the same way. Age, social status, disability, national or ethnic minority background, migrant background, geographic location, and other social disadvantages or prejudices can interact and increase some women's exposure. Preventive and support measures must therefore also take intersecting disadvantages into account.

Building on the Hungarian and comparative research findings of the +3R project, international standards and working good practices, the guidelines aim to provide practical, implementable and clearly addressed recommendations. Wherever possible, the document seeks to identify not only the desired change but also the institution responsible for it, the possible means of implementation, and the criteria for monitoring that change.

Violence against women in politics is not solely a question of the safety or equal treatment of the women concerned. It is a problem of democratic participation: it affects who enters politics, who remains, on what issues and with what visibility they speak, and who can genuinely take part in shaping collective decisions. Self-censorship and the restriction or abandonment of political engagement are therefore not merely individual consequences, but a loss for democratic pluralism and representation.

Political violence can also have a pre-emptive exclusionary effect: it may push women already in politics towards withdrawal or self-censorship, and it may also deter from candidacy and public engagement those who are only considering entering politics.

A core premise of these guidelines is that violence against women in politics is simultaneously a legal, institutional, political and cultural phenomenon. Legal and institutional reform is therefore indispensable, but not sufficient in itself. One of the most important lessons of the Hungarian research is that a significant part of this violence does not appear as an overt attack that is easy to classify legally, but in a grey zone that those affected, their colleagues and institutions often accept as a natural feature of political life.

Action must therefore simultaneously change the environment that normalises violence, provide those affected with a safe means of responding, and create the conditions for institutional accountability.

The intervention logic of the guidelines

The guidelines follow three mutually reinforcing levels of intervention:

Prevention: changing the political and institutional culture, the rules and the operating environment in order to reduce the risk of gender-based political violence emerging and becoming normalised. This includes, among other things, establishing clear standards of conduct, leadership responsibility, training, a safe political and campaign environment, and reducing the structural factors that hinder women's equal political participation.

Protection and response: easily accessible, safe and confidential reporting options, legal, psychological, security and digital support, rapid risk assessment, and a coordinated and proportionate institutional response. The response must not place the entire burden of recognising, documenting and handling the violence on the woman concerned.

Accountability: impartial investigation of reports, foreseeable and proportionate consequences attached to breaches of law or of norms, systematic monitoring of cases and institutional responses, and evaluation of the effectiveness of the measures applied.

The three levels are interdependent. Prevention without consequences can lose credibility, a complaint mechanism without a supportive institutional culture may remain unused, and accountability cannot be verified without adequate data collection and transparent procedures.

This approach also translates the logic of the +3R project into institutional action. Recognise: let us name the forms of political violence and the patterns that normalise it. Resist: let us create a genuine opportunity for safe response, for

seeking help and for institutional intervention. Rise Up: let us transform the norms and structures that allow violence to be reproduced, and create a political environment in which women can not only enter politics but also remain there safely and take on leadership roles.

How can the guidelines be used?

The guidelines are not merely a collection of policy recommendations. They can be used as a practical tool to assess how institutions currently operate, to develop new rules and procedures, and to monitor the implementation of the measures undertaken.

The recommendations can serve as a starting point for, among other things, institutional and party-level codes of conduct, independent complaint and support mechanisms, campaign-security and digital incident-handling protocols, police and judicial procedures and training, institutional self-assessment and gender audits, and the development of regular data-collection and monitoring systems.

The guidelines can be applied at both national and local level. A local government, a local party organisation or a smaller campaign team does not necessarily need the same institutional solutions as Parliament or a national political party, but the minimum requirements of prevention, safe reporting, support and accountability apply at every level.

The document can also be used as an advocacy tool: it helps translate general political commitments into concrete pledges tied to a responsible actor, a specific measure, a timeframe and a measurable outcome.

1.2 Political context

The parliamentary elections of 12 April 2026 significantly reshaped the Hungarian political and institutional environment. The TISZA Party won 141 seats in the 199-member Parliament, Fidesz-KDNP obtained 52 and Mi Hazánk 6 seats. The start of the new parliamentary term creates an opportunity to review institutional rules, procedures and political norms, and these guidelines therefore identify several measures that can be implemented in the short or medium term.

The parliamentary elections of 12 April 2026 significantly reshaped the Hungarian political and institutional environment. The new parliamentary term creates an opportunity to review institutional rules, procedures and political norms, and the guidelines therefore identify several measures that can be implemented in the short and medium term.

For a long time, violence against women in politics remained virtually invisible in Hungary as a distinct policy and institutional problem. Data from the institutions contacted within the +3R project revealed no functioning monitoring or complaint-handling system specifically tracking gender-based violence in politics. This stands in sharp contrast to the research findings, according to which numerous forms of the phenomenon are present in the political sphere, while a significant proportion of cases remain unreported and unrecorded by institutions.

The recommendations apply to all political actors and institutions regardless of party affiliation; their aim is to define lasting minimum standards that remain applicable irrespective of changes in government or politics.

Why now?

- A new institutional cycle: an opportunity to embed new parliamentary, governmental and party-level norms and mechanisms.
- EU legal harmonisation: the transposition deadline for Directive (EU) 2024/1385 is 14 June 2027.
- International benchmarks: the Istanbul Convention and other international standards can also be used to assess domestic regulation.
- Available knowledge: building on the +3R research, the comparative findings, the trainings and the good practices of partner countries, the next step can already be the development and implementation of concrete measures.

1.3 Hungary compared with the +3R partner countries

Dimension	Hungary's position
Parliamentary representation	The share of women in Parliament has reached 25%, similar to the representation figures for Slovakia, Czechia and Ireland. In Germany the share of women members is 35%. It nonetheless still falls short of the EU Member State average (33.6%).
Institutional complaint mechanism	There is no independent parliamentary complaint and support mechanism established to address gender-based political violence; institutional data for the period examined revealed no proceedings recorded under such a category.
Istanbul Convention	The other four project countries have ratified the Istanbul Convention; Hungary signed it in 2014 but has not ratified it.

Dimension	Hungary's position
Legal category	VAWP is not a distinct legal category. Nor does VAWP appear as a unified, standalone legal category in the other project countries; the related conduct is addressed by various criminal-law, labour-law, anti-discrimination and other rules.
Online harassment	The legal framework (Section 332/A of the Criminal Code) addresses certain forms of online attack, but it is not VAWP-specific and is not built on a consistent gender-sensitive approach. Partner countries operate different legal, platform-regulation and civil-society support solutions, from which several adaptable good practices can be identified.

1.4 Key findings of the +3R research and the forms of violence

The Hungarian research ("The Limits of Tolerance", WP3, n=11) and the comparative results from the five countries together provide the empirical basis of the guidelines. The Hungarian qualitative sample is not generalisable on its own, but the data from the partner countries confirm the systemic nature of the patterns identified.

In the comparative report, online violence was the most frequent (96.8%), followed by psychological (87.4%), sexualised (53.7%), physical (33.7%) and economic violence (30.5%). In the Hungarian sample, online and psychological violence each appeared in 91% of cases. In every country studied, the number of reported cases fell significantly short of the violence actually experienced.

The Hungarian research identified six interrelated mechanisms:

- normalisation: violence becomes a tacit part of political life;
- personalisation and depoliticisation: instead of political content, the attack targets the woman's person, body or gender;
- accumulation: online, offline, institutional and private spaces become interconnected;
- structural embeddedness: party structures, informal networks and procedures can also sustain exclusion;
- coordinated attack patterns: media attacks and disinformation campaigns can reinforce one another;
- self-perpetuating spiral: the absence of consequences can encourage further attacks.

In the research, sexist and humiliating conduct came not only from external actors but also from fellow representatives and from within political organisations. This justifies placing institutional culture and internal rules, alongside legal protection, at the centre of the recommendations.

The main forms of violence

Online violence: threats, harassing messages, manipulated or sexualised content, doxxing and coordinated attacks. Online violence can also extend to the private sphere and to family members, and can escalate into a physical security risk.

Psychological violence: sexist or sexualised remarks, humiliation, intimidation and threats. Its particularly high prevalence in the Hungarian sample points to a hostile political environment.

Sexualised violence and harassment: unwanted sexual remarks, advances and other sexualised attacks. These are often normalised in the "grey zone" between legitimate political debate and harassment.

Physical violence and threats: rarer, but because of its seriousness it requires early risk assessment and recognition of the signs of escalation.

Economic violence and institutional pressure: restricting access to resources, information, speaking opportunities, positions or staff capacity. Transparent regulation and monitoring of such decisions is needed.

The forms of violence are often interconnected, and age, background, disability or other social circumstances can further increase exposure. Risk assessment and the institutional response must therefore examine not isolated incidents but the overall pattern.

Policy implication: VAWP cannot be addressed solely at the level of individual incidents or criminal proceedings. Action must simultaneously address institutional conduct, the functioning of parties, the online space, law enforcement and political culture, in line with the threefold logic of prevention, protection and response, and accountability.

2. European and international legal framework

2.1 The EU Directive on violence against women (2024/1385)

Full reference: Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence (OJ L, 2024/1385, 24.5.2024). The Directive is the EU's first

comprehensive, binding legislative act in this field. Member States must bring into force the national provisions necessary to comply with the Directive by 14 June 2027.

The Directive requires the EU-wide criminalisation of several acts that are directly relevant to violence against women in politics. These include the non-consensual online sharing of intimate or manipulated material, cyberstalking, cyberharassment (including certain coordinated online attacks), the sending of unsolicited sexual material and the malicious disclosure of personal data, as well as incitement to gender-based online violence or hatred.

This is a particularly significant development for women in politics. The preamble to the Directive expressly recognises that widespread and coordinated online attacks often target prominent women politicians, journalists and human-rights defenders, and that online violence can also escalate into offline attacks.

Article / element	Content relevant to VAWP
Article 5	Criminalisation of the non-consensual sharing of intimate or manipulated material. This may include, among other things, sexual manipulated or deepfake material created or disseminated to discredit women politicians, where it meets the conditions set out in the Directive.
Article 6	Cyberstalking: the repeated or continuous, unauthorised surveillance of a person's movements or activities using ICT means.
Article 7	Cyberharassment: including threatening online conduct, publicly threatening or abusive attacks carried out jointly with others, the sending of unsolicited sexual content and, in specified cases, the malicious disclosure of personal data.
Article 8	Criminalisation of incitement to online violence or hatred against a group defined on the basis of gender, or a member of such a group.
Article 14	Accessible, easy-to-use and safe reporting channels. For the cybercrimes under Articles 5-8, the possibility of online or other secure digital reporting and submission of evidence must be ensured.
Article 15	Bodies conducting investigation and prosecution must have appropriate expertise and effective investigative tools, in particular for the collection, analysis and preservation of electronic evidence.
Preamble	The Directive recognises that widespread, coordinated online harassment attacks frequently target prominent women politicians, journalists and human-rights defenders.
Victim protection and support (several related provisions)	The Directive requires an assessment of victims' individual needs and risks, access to appropriate support and protection measures, and, in specified circumstances, consideration of the protection of children.

2.2 Connection to the Digital Services Act (DSA)

Regulation (EU) 2022/2065 on a Single Market for Digital Services (the Digital Services Act, DSA) sets out the EU framework for the operation of digital platforms, the handling of illegal online content and the mitigation of systemic online risks. Together with Directive 2024/1385, it therefore provides an important legal framework for addressing online violence against women in politics.

For violence against women in politics, it is not only the removal of individual illegal content that is relevant. Coordinated waves of harassment, the disclosure of personal data, the dissemination of manipulated sexual content and algorithmic amplification can create systemic risks, in the management of which platforms, national authorities and EU institutions all have a role.

The Hungarian policy response must therefore extend, alongside criminal-law regulation, to the effective use of the reporting, supervisory and risk-mitigation tools available under the DSA.

At the same time, the DSA does not create a separate "violence against women in politics" category, and does not automatically render unlawful all sexist, humiliating or politically motivated content. Its significance lies in the fact that, alongside the handling of individual infringements, it also creates a point of connection to platforms' systemic risk-management and transparency obligations.

2.3 The significance of EU legal harmonisation for violence against women in politics

The transposition of Directive 2024/1385 is not merely a technical harmonisation task for Hungary. It creates an opportunity for Hungarian law and institutional practice to recognise and address more consistently those forms of online violence that, according to the +3R research, particularly frequently affect women in politics.

During transposition it must therefore be examined specifically whether Hungarian regulation and law enforcement adequately cover the non-consensual dissemination of intimate and manipulated content, cyberstalking, coordinated online attacks, the malicious disclosure of personal data and incitement to gender-based online violence or hatred.

Harmonisation, however, cannot be limited to creating new criminal offences or amending existing ones. Implementation of the Directive also affects reporting options, victim support and protection, risk assessment, police and judicial capacity, the handling of electronic evidence, prevention, and data collection and monitoring.

The transposition deadline of 14 June 2027 therefore creates a concrete policy and advocacy opportunity. The +3R research findings and recommendations can be used to examine the extent to which transposition responds to the specific forms of violence affecting women in politics and to the institutional obstacles they face.

Minimum aspects to examine during transposition

During the transposition of Directive 2024/1385 in Hungary, at least the following aspects should be examined:

- adequate criminal-law coverage of the relevant forms of gender-based online violence;
- a safe and easily accessible online reporting option;
- ensuring the easy submission, preservation and official handling of electronic evidence;
- pattern-based risk assessment of repeated, coordinated or escalating online attacks;
- consideration of the safety of the victim and, where necessary, their family members;
- ensuring appropriate police, prosecutorial and judicial expertise;
- the meaningful involvement of civil-society and victim-support organisations in shaping transposition and implementation;
- the development of data collection disaggregated by sex and capable of identifying the forms of online violence.
- examining whether the reporting, risk-assessment and support mechanisms are genuinely accessible also to elected officials, candidates, political staff and local public figures.

Responsibility and monitoring: in preparing transposition, alongside the involvement of the state bodies responsible for legislation, justice, victim protection and law enforcement, the meaningful participation of women's-rights and victim-support civil-society organisations and of experts on online violence must be ensured. After transposition, it must be regularly assessed whether the new or amended rules have in practice improved the accessibility and effectiveness of reporting, protection, investigation and support.

2.4 The lack of ratification of the Istanbul Convention

In 2014 Hungary signed the Council of Europe Convention on preventing and combating violence against women and domestic violence (Istanbul Convention, CETS No. 210), but has not ratified it to date. In May 2020 the Parliament, in a political declaration, rejected support for ratification, citing among other things the Convention's concept of gender and certain provisions on asylum.

The European Union acceded to the Convention in 2023, and it entered into force for the EU on 1 October 2023. EU accession creates obligations for the Union within the limits of EU competences, but it does not replace Hungary's own ratification.

The lack of ratification of the Istanbul Convention is not merely a symbolic question.

Hungary is not bound by an obligation, arising from the Convention as a whole, to ensure the prevention of violence against women, the protection and support of victims, the accountability of perpetrators and coordinated policy action within the comprehensive framework defined by the Convention. Even in the absence of ratification, however, the Convention remains an important policy benchmark for assessing domestic regulation and institutional practice. Ratification continues to require a separate Hungarian political and legislative decision.

Article	Content
Article 33	Psychological violence - seriously impairing a person's psychological integrity through coercion or threats
Article 34	Stalking: criminalisation of repeated threatening conduct directed at another person that causes them to fear for their safety.
Article 35	Physical violence
Article 36	Sexual violence, including non-consensual sexual acts
Article 40	Sexual harassment - unwanted verbal, non-verbal or physical conduct of a sexual nature that creates a degrading, hostile or intimidating environment

These provisions of the Convention were not drafted specifically for political actors, but they cover several forms of violence that the +3R research also identified among women in politics.

2.5 CEDAW: women’s political participation and protection against gender-based violence

Hungary ratified the UN Convention on the Elimination of All Forms of Discrimination against Women (CEDAW) in 1982. Article 7 of the Convention obliges States Parties to eliminate discrimination against women in political and public life and to ensure women’s equal participation in elections, public policy-making and the holding of public office.

General Recommendation No. 23 of the CEDAW Committee deals specifically with women’s participation in political and public life. General Recommendation No. 35 sets out States’ obligations regarding gender-based violence. General Recommendation No. 40, adopted in 2024, treats women’s equal and inclusive representation in all decision-making systems as a fundamental democratic requirement, and emphasises the need to remove structural barriers and intersecting disadvantages.

In its 2023 concluding observations on Hungary’s ninth periodic report, the Committee specifically addressed women’s participation in political and public life. Among other things, it urged targeted measures to increase women’s representation in decision-making, as well as measures to counter negative attitudes, discriminatory conduct and hate speech against women in politics.

CEDAW is therefore relevant to these guidelines from two directions: it requires the elimination of political discrimination against women and of their under-representation, and it requires effective state action against gender-based violence. Violence against women in politics lies at the intersection of these two obligations.

The common message of the European and international framework

The EU Directive on violence against women, the DSA, the Istanbul Convention and CEDAW are instruments of different legal nature and scope, but for violence against women in politics they point in a common direction. Effective action cannot be limited to criminal accountability: it requires prevention, safe reporting and support options, appropriate institutional and official capacity, risk assessment, data collection, and the safeguarding of women’s equal and safe political participation.

The next chapter examines the extent to which the current Hungarian legal framework is able to meet these requirements, and where regulatory or enforcement gaps remain.

3. National legal framework

Several provisions of current Hungarian law can be applied to particular manifestations of violence against women in politics, but VAWP does not appear as a distinct legal category, and the application of the relevant provisions does not form a coherent system of protection.

Legislation	Relevant provision
Act C of 2012 (Criminal Code), Section 195	Coercion - preventing others from exercising their rights through violence or threats
Criminal Code, Section 216	Violence against a member of a community: violent, threatening or defiantly antisocial conduct as defined by law, committed on account of a person’s real or presumed belonging to a specified group or to certain groups of the population. “Sex” does not appear as a distinct protected category in the illustrative list of the offence, so attacks motivated by belonging to the female sex do not automatically fall under this provision.
Criminal Code, Section 222	Harassment - persistent conduct that instils fear or is threatening or disturbing
Criminal Code, Sections 226-227	Defamation and libel - according to judicial practice, public figures are subject to a heightened duty of tolerance
Criminal Code, Section 332/A (2025)	Online aggression: the expression, before a wide audience on an electronic network, of an intention or wish to commit a violent crime causing death or committed with particular cruelty against an identifiable person or persons. A gender-neutral offence that may be applied to certain serious forms of online violence against women in politics.
Act CXXV of 2003 (Equal Treatment Act), Section 10	The definition of harassment - conduct connected to a protected characteristic (e.g. sex) that violates human dignity and creates an intimidating or degrading environment
Act LXXVIII of 2024 on curbing online aggression	In addition to inserting Section 332/A into the Criminal Code, it also introduced rules on handling unlawful comments appearing in the comment sections of online press products. The regulation does not apply a gender-sensitive approach.

The provisions listed regulate different legal subject matters and forms of conduct, and none was drafted specifically for the complex phenomenon of violence against women in politics. Some VAWP cases may therefore become the subject of criminal, civil or equal-treatment proceedings, while other conduct may not necessarily reach the threshold required to apply the given legal provisions.

The legal handling of cases in which several acts of individually differing gravity together form a sustained or coordinated pattern of attack can be particularly difficult. Online harassment, sexist or sexualised attacks, the disclosure of personal data, threats and political discrediting can reinforce one another, while current law examines them under separate legal categories.

The offence of online aggression, in force since 2025, created a new criminal-law tool for a narrow, serious range of online violence, but it is not a general offence of online harassment or gender-based violence. The fragmentation of the regulation therefore does not necessarily call for the creation of a new standalone offence, but above all for an examination of whether the existing substantive, procedural and institutional tools are together able to recognise and effectively address the specific patterns of violence against women in politics.

3.1 Distinguishing political criticism from gender-based attack

Freedom of expression and the open discussion of public affairs are fundamental democratic rights. Hungarian law therefore expects public figures, including politicians, to tolerate a wider range of criticism in connection with the debate of public matters. This does not mean, however, that public figures are left without protection under personality-rights or criminal law.

Under Section 2:44 of the Civil Code, the fundamental rights ensuring the free discussion of public affairs may restrict the protection of a public figure's personality rights only to a necessary and proportionate extent, and without violating human dignity. In respect of communications or conduct falling outside the debate of public affairs, a public figure is entitled to the same protection as a non-public figure; and their private and family life does not in itself constitute a public matter.

From the perspective of violence against women in politics, the aim is therefore not to abolish the higher threshold of tolerance applicable to public figures, but to draw a consistent distinction between what falls within legitimate political criticism and what constitutes gender-related humiliation, threat, sexualised attack, harassment or other unlawful conduct that is no longer aimed at contesting a political position.

From this perspective the +3R research points to an important problem: part of the attacks on women politicians is formally linked to political conflict, but in substance targets the person's gender, body, sexuality, family role or private life. To assess such cases properly, it is not enough to examine merely whether the attack occurred in a political context; its content, purpose, repetition, gravity and any threatening or silencing effect must also be taken into account.

Recommendation: Clearer criteria should be developed in enforcement practice for distinguishing legitimate political criticism from gender-based attack. The assessment should take into account in particular the political relevance of the communication, its gendered or sexualised nature, its repetition, its threatening or intimidating effect, the interconnection of online and offline conduct, and whether the attack is capable of restricting or rendering impossible the person's political participation.

3.2 Legal protection beyond criminal law

Addressing violence against women in politics cannot be limited to criminal law. Much conduct that does not reach the statutory threshold of a criminal offence may infringe personality rights, may amount to gender-based harassment, discrimination or unlawful data processing. Effective protection therefore requires that criminal-law, civil-law, equal-treatment and data-protection tools be treated as a mutually complementary system.

Personality-rights protection: The personality-rights rules of the Civil Code provide protection against, among other things, the violation of human dignity, honour and reputation, private and family life, the home, and the right to the protection of personal data. This can be particularly relevant to violence against women in politics in cases of sexist or sexualised discrediting, attacks targeting private life or family members, or the unlawful disclosure of personal data. The higher threshold of tolerance applicable to public figures does not mean the loss of these rights.

Equal treatment and harassment: Equal-treatment legislation prohibits harassment connected to a protected characteristic, including sex, in the fields and legal relationships to which the law applies. This can be a relevant avenue of protection, for example in institutional or employment situations where gender-based conduct creates an intimidating, hostile, degrading, humiliating or offensive environment. However, this avenue cannot be applied automatically to every political or public-life conflict; the personal and material scope of the legislation must be examined in each case.

Data-protection remedies: Online attacks on women in politics may also involve the unlawful processing of personal data. The malicious disclosure of personal data concerning a person's home address, contact details, family members or

children can pose a particularly serious security risk. Under data-protection rules, the data subject may, depending on the circumstances of the case, request the erasure of their personal data or the restriction of processing, object to the processing, or, in the event of an infringement, turn to the competent data-protection authority.

Data-protection law, however, does not provide general protection against all doxxing or online attacks. Unlawfulness must be assessed with regard to the nature of the data and the legal basis, purpose and circumstances of the processing.

One fundamental problem of the current system is the fragmentation of the avenues of legal protection. Criminal-law, civil-law, equal-treatment, data-protection and platform-level remedies belong to different forums and can be pursued under different conditions. In the case of a complex or repeated series of attacks, a significant burden may therefore fall on the person concerned in identifying what legal remedies are available, which forum to turn to, what evidence to preserve, and what proceedings may be initiated.

Recommendation: An easily accessible, independent first point of contact and advice should be ensured which, in the case of attacks on women in politics and public life, helps with the initial assessment of the case, the identification of the available avenues of legal protection, the preservation of evidence, and referral to the appropriate authority or to legal, victim-support or other support services. This function need not be created as a new, parallel institution: it can be built into the independent complaint and support mechanism proposed in these guidelines.

4. Police and judicial proceedings

Effective legal protection against violence against women in politics depends not only on whether an applicable law exists, but also on whether the person concerned actually has access to that protection, whether the authority recognises the nature and gravity of the attack, whether it properly assesses repeated or escalating conduct, and whether the proceedings avoid causing further, preventable burden or harm.

The experiences of the women who spoke in the Hungarian +3R research indicate a significant gap between the legal tools formally available and their use in practice. Recurring themes in the interviews were the fear that reporting would be futile, the absence of an institutional response, and the experience that attacks accompanying political engagement are treated as part of the higher tolerance expected of the person concerned.

Several interviewees reported that, when they made a police report, the higher tolerance expected of public figures was invoked, even in matters where, according to the person's account, a threat or an attack directed at family members or children was also present. This is particularly problematic, because the broader tolerance expected in the debate of public affairs is not the same as an obligation to tolerate threats, harassment or other unlawful conduct.

The research does not, however, allow the conclusion that this is a uniform nationwide police or judicial practice. The cases revealed in the interviews indicate the need for a targeted examination of enforcement practice, and for ensuring that the political context alone does not lead to an underestimation of the dangerousness or the gendered nature of the attack.

4.1 The limits of an incident-based approach

One characteristic of violence against women in politics is that individual acts often build on one another. A sexist comment, a threatening message, repeated online harassment, doxxing or the contacting of family members may each fall under a different legal assessment on its own, but together they can form an escalating pattern of attack that endangers both the person's safety and their political participation.

The assessment by authorities cannot therefore be limited solely to the most recently reported event. Where the circumstances of the case so warrant, it is necessary to examine the antecedents, the repetition, the connection between conduct appearing across different communication channels and in physical space, the signs of escalation, and whether the attack extends to the person's family members or private life.

This is particularly important in the case of online violence. Digital threats cannot automatically be treated as less serious merely because they occur online. Cyberstalking, doxxing, repeated threats and the use of personal data may in some cases also signal the emergence of a physical security risk.

4.2 Territorial jurisdiction and effective access to proceedings

Because of the specific features of acts committed online, the perpetrator, the person concerned and the effect of the attack may be linked to different geographic locations. If, during the proceedings, the person concerned has to appear repeatedly in person before an authority far from their home or place of work, this can cause a significant burden of time, money and psychological strain.

Procedural practice must therefore, within the limits of current law, reduce as far as possible the unnecessary burden falling on the person concerned. Where possible, it must be ensured that a hearing or other procedural act can take place at a location accessible to the person concerned, or remotely by appropriate technical means.

The handling of online cases also requires effective cooperation between the police and other authorities involved. The application of jurisdictional rules must not result in the person concerned effectively bearing the burdens of the geographic operation of the procedural system.

4.3 Risk assessment and safety

In assessing the gravity of a threat, it is not enough to examine only the text of individual communications. Particular attention is required for repeated or intensifying threats, following, the acquisition or disclosure of personal data, knowledge of information about the person's physical whereabouts, and the involvement of family members or children.

In such cases a standardised, documented risk assessment is needed, on the basis of which the necessary protective, investigative and support measures can be determined. The risk assessment must be reviewed in the event of new information, a change in the perpetrator's conduct or an escalation of the violence.

4.4 Handling digital evidence

Proving online violence requires specific expertise. Offensive or threatening content can be deleted, altered, moved to another platform or widely disseminated within a short time. It must therefore be possible to record, submit, preserve and assess electronic evidence properly.

Easily accessible information must be provided to those affected on how to document online attacks safely. The burden of collecting evidence cannot, however, be placed entirely on the victim. The police and other competent bodies must have appropriate expertise and technical capacity to handle electronic evidence.

This is also directly linked to the implementation of Directive (EU) 2024/1385, which requires safe reporting options and adequate official capacity for the forms of online violence falling within its scope.

Recommended procedural minimums

- Accessible reporting: the person reporting must not suffer an unjustified disadvantage because the authority handling the case is geographically distant. Where legally and technically possible, local or remote hearing must be ensured.
- Pattern-based assessment: repeated threats, harassment and online attacks must be assessed not only as isolated events but also as part of a possible escalating pattern of attack.
- Standardised risk assessment: in cases of serious or repeated threats, stalking, doxxing, or threats against family members or children, a documented risk assessment must be applied.
- Digital evidence: the conditions for the easy submission, professional recording, preservation and assessment of electronic evidence must be ensured.
- Expertise: it must be ensured that appropriately trained professionals familiar with the specific features of violence against women in politics and of online violence can, where necessary, be involved in handling cases.
- Preventing secondary victimisation: during the proceedings, unnecessary repeated hearings, victim-blaming communication and procedural burdens that are not necessary for investigating the case must be avoided.
- Proper assessment of the political context: the broader tolerance of criticism expected of public figures cannot in itself serve as grounds for rejecting a report made on account of a threat, harassment or other unlawful conduct.
- Monitoring: the competent bodies must develop data collection that makes it possible to examine the relevant forms of gender-based violence, online commission, repeated attacks and the outcomes of proceedings, while ensuring the protection of personal data.

5. Institutional capacity and digital protection

Online violence is one of the most frequent findings of the +3R research, and it places a significant, often invisible workload on those affected, their communications staff and their assistants. Monitoring, documentation, contact with platforms and risk assessment cannot therefore be regarded as the responsibility of the individual user alone.

5.1 Institutional digital-security minimums

Political institutions, parties and parliamentary groups should ensure:

- minimum standards for secure use of accounts and devices;

- a consistent method for documenting online threats and preserving evidence;
- protection of personal and family data;
- a designated incident contact person and a rapid escalation route;
- where necessary, legal, IT, psychological and security expert support.

Support must also be accessible to local and regional politicians, local-government candidates and smaller organisations.

5.2 Rapid response and doxxing

In cases of serious, repeated or coordinated attacks, digital and physical risks must be assessed together. Threats of death or bodily harm, stalking, doxxing, manipulated or sexualised content, and the targeting of family members or children require a priority response.

Where data concerning a person's home address, contact details or family members is disclosed with harmful intent, the preservation of evidence, support for takedown requests to platforms, risk assessment and, where necessary, reporting to the authorities must be ensured. In the legal assessment, however, it must be taken into account that certain data of public figures may lawfully be public.

5.3 Moderation and technical capacity

Automated or semi-automated moderation, and tools that help filter threatening content and detect coordinated attacks, can reduce the burden on those affected. TrollWall-type solutions identified by the Czech partner provide an adaptable example, but they do not replace the platforms' and institutions' own responsibility, and their use requires data-protection, transparency and redress safeguards.

5.4 Platform responsibility and the DSA

The DSA connects to the online forms of VAWP through obligations on reporting, transparency and systemic risk management. Institutional practice must extend not only to reporting individual content but also to recognising coordinated attacks, manipulated content, doxxing and other systemic risks. In serious or recurring cases, maintaining contact with platforms and with the competent national or EU bodies is an institutional task.

Recommendations: consistent digital-security and incident-handling minimums; recognition of the additional workload in terms of capacity and budget; support for local actors; a rapid escalation protocol; making technological tools accessible; in the case of doxxing, rapid documentation and risk assessment; institutional contact with platforms; and regular, anonymised monitoring.

6. Training and preparation of the police and the judiciary

Effectively addressing violence against women in politics requires not only appropriate laws and procedural protocols but also professionals able to recognise the specific patterns of gender-based, political and digital violence. This is particularly important for actors in the police, the prosecution service and the judiciary, whose decisions directly affect whether those concerned actually have access to legal protection.

The interviews in the Hungarian +3R research suggest that the experiences of those concerned can differ significantly depending on how the professional handling the case interprets the political context, the broader tolerance of criticism expected of public figures, the gravity of online threats, or the connection between repeated attacks. The aim of training is therefore not merely to convey general knowledge about gender-based violence, but to develop a more uniform and consistent enforcement practice.

It is particularly important to recognise that the context of political conflict does not in itself reduce the gravity of a threat, harassment or other unlawful conduct. Likewise, commission online does not automatically mean that the attack is less dangerous. Training must help distinguish what falls within legitimate, even sharp, political criticism from cases where elements appear that may warrant legal or security intervention.

6.1 Minimum content of the training

The training of the relevant actors in the police, the prosecution service and the judiciary should cover at least the following areas:

- Recognising VAWP: the concept and specific features of violence against women in politics and its connection to women's political participation.

- Distinguishing legitimate political criticism from unlawful attack: alongside protecting freedom of expression, the proper recognition of threatening, harassing, sexualised or other unlawful conduct.
- Pattern-based assessment: recognising that several events of individually differing gravity can together form a repeated or escalating pattern of attack.
- Online violence: cyberstalking, coordinated online harassment, doxxing, sexual or manipulated content, threats, and the risk of online attacks escalating offline.
- Risk assessment: proper assessment of repetition, escalation, the acquisition of personal data, physical proximity, and the involvement of family members and children.
- Digital evidence: the basic requirements for recording, preserving, assessing and using electronic evidence in proceedings.
- Preventing secondary victimisation: appropriate communication, avoiding victim-blaming, and reducing unnecessary repeated hearings and other avoidable procedural burdens.
- Legal and institutional avenues: knowing which civil-law, data-protection, victim-support or other protective options may be relevant alongside the criminal-law handling of the case.

6.2 Not one-off awareness-raising, but professional competence

Training cannot be limited to one-off, general awareness-raising programmes. The knowledge needed to address VAWP must be built into the relevant basic and continuing training systems of the police, the prosecution service and the judiciary.

Training must be role-specific. Police officers primarily need competence in properly receiving a report, recognising risk, securing evidence and taking the necessary measures. For prosecutors, the legal assessment of evidence and of the pattern of attack is key; for judges, among other things, the proper application of the boundary between the protection of political expression and unlawful conduct may be of particular importance.

Training should also be based on practical cases, scenarios and decision-making situations. The anonymised cases from the +3R research can provide a suitable training basis for this.

6.3 Protocol and professional support

Training alone is not sufficient if the professional handling a case has no practical protocol or professional support to turn to in a specific matter.

It is therefore warranted to:

- develop short, practical procedural guides;
- apply standardised risk-assessment criteria;
- provide a guide on handling digital evidence;
- ensure the availability, where necessary, of an appropriately trained expert or designated contact person;
- provide the possibility of professional consultation for complex or high-risk cases.

The aim is not necessarily to create new organisational units, but to ensure that the necessary expertise is genuinely available within the system.

6.4 Measuring the impact of training

The effectiveness of training cannot be measured solely by the number of trainings held or participants. It must also be examined whether the knowledge acquired appears in procedural practice.

To this end, the following should be regularly assessed, among other things:

- changes in the knowledge and competence of the professionals who took part in the training;
- the application of risk assessment and digital-evidence handling;
- the duration and outcome of case handling, where such data are lawfully and appropriately anonymised and available;
- the experiences of those concerned regarding the proceedings;
- problems indicating secondary victimisation;
- recurring professional shortcomings that require further training or a modification of the protocol.

Recommendations

- VAWP and online gender-based violence should be incorporated into the relevant basic and continuing training of the police, the prosecution service and the judiciary.
- Training should be role-specific, based on practical cases and regularly renewed.

- Training programmes should be linked to the procedural minimums set out in Chapter 4, in particular pattern-based assessment, risk assessment, digital-evidence handling and the prevention of secondary victimisation.
- It is warranted to involve experts and civil-society organisations working on gender-based violence, victim support, digital security and fundamental rights in the design of the training.
- The effectiveness of training should be assessed not only by participation data but also by indicators examining changes in enforcement practice.

7. Political and institutional culture: from recognition to change

Legal reform, appropriate procedures and complaint mechanisms are necessary but not sufficient on their own. The Hungarian +3R research shows that a significant part of the conduct restricting women's political participation appears in a range that does not necessarily reach the threshold of an infringement, yet can have a repeatedly humiliating, excluding, intimidating or silencing effect. Such experiences are often normalised by those affected, their colleagues and the institutions themselves as a natural feature of political life.

Changing institutional culture therefore requires three mutually reinforcing steps: recognising the problematic patterns, resisting their normalisation, and then creating an institutional and community environment in which the person attacked is not left alone, and in which women's political participation does not become a personal security risk.

This is the cultural and institutional counterpart of the Recognise - Resist - Rise Up approach.

7.1 RECOGNISE - Recognising and naming

One obstacle to recognising violence against women in politics is that, alongside clear threats and physical attacks, much conduct appears whose assessment is less clear-cut in itself. This may include recurring remarks about appearance, age or sexuality, unwanted physical proximity, persistent interruption, exclusion from informal decision-making, the consistent devaluation of professional performance, or the appropriation of ideas. These experiences recurred throughout the Hungarian research.

Not all such conduct constitutes violence or an infringement in itself. Its policy significance becomes particularly strong when it appears on a gendered basis, repeatedly or as an institutionalised pattern, and restricts the person's opportunities to speak, decide or participate.

The aim of recognition is therefore not to classify political conflict or every unpleasant interaction as "violence". The aim is to recognise when a gendered pattern emerges behind particular conduct that places women under a different or greater burden of adaptation.

"As a woman, you have to balance on a narrow path from the outset: you cannot be too weak, but not too aggressive either, while constantly having to prove your fitness for leadership."

Hungarian woman member of parliament

Recognising normalising language

The persistence of problematic conduct is often aided by phrases that make it seem natural or insignificant:

"It's part of politics."

"If you're a public figure, put up with it."

"It was just a joke."

"Don't be so sensitive."

"Male politicians get attacked too."

These phrases do not in themselves prove that violence has occurred. They may, however, serve to close down the conversation instead of examining the case on its merits. The institutional response must therefore examine not the person's sensitivity, but the content, context, repetition, gendered nature, effect and possible escalation of the conduct.

7.2 RESIST - Resisting normalisation

Recognition must be followed by an institutional response. It is not enough for the person concerned to recognise that conduct is unacceptable; political institutions, parties, parliamentary groups and local governments must also make clear what standards of conduct they expect.

Resistance does not mean only a formal complaint or disciplinary procedure. Early, low-threshold intervention can in many cases prevent the conduct from recurring or worsening.

Such intervention may include:

- immediately naming the problematic conduct;
- public or personal support for the person attacked;
- a signal or warning from leadership;
- providing confidential consultation;
- application of the code of conduct;
- in the event of repetition, a formal complaint or disciplinary procedure;
- in the case of a threat or security risk, immediate escalation to the appropriate institutional or official level.

The role of witnesses and colleagues is particularly important. Institutional culture changes when the responsibility for responding does not fall solely on the woman who is attacked.

7.3 RISE UP - Solidarity, retention and political participation

The consequence of violence against women in politics is not only individual harm. According to the +3R research, attacks can influence how much women speak, which issues they take on, whether they seek another candidacy or leadership role, and, in the longer term, whether they remain in politics.

The aim of action therefore cannot end with the closure of an incident. The institutional response must also help the person concerned to continue their political or public activity safely.

This may require professional, legal and psychological support, mentoring, security assistance, and visible solidarity from colleagues and leaders. Particular attention must be paid to those with fewer institutional resources, such as local and regional politicians, first-time candidates, young women, representatives of smaller parties or organisations, and women exposed to intersecting disadvantages.

Solidarity must also be able to cross party lines. The rejection of threats, sexual harassment or gender-based violence against women cannot be made dependent on which political side the person concerned belongs to.

Cross-party women's and allies' networks, the sharing of experience, mentoring and public norms should therefore be supported, making clear that sharp debate with a political opponent is legitimate, while gender-based violence is not a political tool.

7.4 Regular self-assessment of institutional culture

Change in institutional culture cannot be measured solely by the number of reported cases. A low number of reports may mean few incidents, but it may also indicate a lack of trust, of a safe reporting option, or of recognition.

Parliamentary groups, political parties and larger local governments should therefore assess their own functioning at least once a year from the perspective of the risks of violence against women in politics.

The self-assessment should cover at least the following areas:

- organisational culture and leadership conduct;
- the awareness and accessibility of reporting and consultation options;
- fear of retaliation;
- the institutional response to cases;
- digital and campaign security;
- women's participation in formal and informal decision-making;
- the functioning of training and preventive measures;
- the implementation of the measures undertaken since the previous assessment.

The aim of self-assessment is not to "rate" an organisation, but to recognise risks early and develop a concrete action plan. The results must be discussed at leadership level, and the implementation of the measures undertaken must be reviewed in the next assessment.

Recommendations

- The recognition of ambiguous, repeated and normalised gender-based conduct should feature in the training and internal rules of political institutions and parties.
- The institutional response should not be triggered only by a formal complaint: there should be scope for early, low-threshold intervention and confidential consultation.
- The responsibility of leaders and witnesses should be expressly reflected in the standards of conduct.

- The aim of post-attack support should be not only to close the case, but to maintain the person's safe political participation.
- Cross-party forms of solidarity, mentoring and women's cooperation should be supported.
- Political parties, parliamentary groups and larger local governments should introduce regular institutional self-assessment, with a concrete action plan and follow-up.

8. Standards of acceptable conduct

Sharp criticism and conflict are inherent in political debate. The aim of action against VAWP is not to restrict this, but to separate legitimate political criticism from gender-based humiliation, threats, harassment and violence.

8.1 Minimum standard and scope

The written standards of conduct of Parliament, parliamentary groups, parties, local governments and other political institutions should name at least the following: gender-based insult and sexualised remarks; unwanted sexual advances; threats and harassment; gender-based online attacks; manipulated or sexualised content; doxxing; the involvement of family members; and retaliation.

The rules should cover, in addition to official sittings, campaigns, events, travel, internal communication and the online space connected to the political role, and—depending on the nature of the institution—leaders, members, candidates, staff, advisers, campaign teams and volunteers.

8.2 Consequences and protection against retaliation

A standard is workable only if its breach carries foreseeable, transparent and proportionate consequences. Gravity, repetition, power differential, harm caused, security risk and retaliation must be assessed together. The perpetrator's political position or electoral significance cannot justify the absence of an investigation or a more lenient assessment.

A person who makes a complaint, acts as a witness or provides support must be protected against political, professional and informal retaliation; retaliation must be treated as a separate breach of the norms.

8.3 Leadership and parliamentary responsibility

Leaders are responsible for the standards being known, for their own consistent conduct, for the substantive handling of serious cases, and for ensuring that the institution's reputation does not override the safety of the person concerned.

In Parliament, a gender-sensitive standard of conduct clearly extending also to members is warranted, with a clear complaint-handling procedure, consequences, protection against retaliation and anonymised monitoring. The presiding officer's immediate power to maintain order and the investigation of a formal complaint are separate functions.

8.4 The Male Pledge and review

The +3R Male Pledge, as a voluntary entry point, can support a shift in norms and a public commitment to institutional reforms, but it does not replace binding rules, a complaint mechanism or sanctions.

The application of the standards of conduct must be reviewed at least once per electoral cycle, and after any significant incident or change in the law.

9. Political parties and campaigns

Political parties play a decisive role in the conditions under which women can enter politics, the opportunities they have for political advancement, the environment in which they can do their work, and the protection they can expect if they experience gender-based violence.

The Hungarian +3R research also showed that violence against women in politics does not come solely from political opponents or unknown online perpetrators. Power relations within parties, parliamentary groups and political institutions, informal networks, loyalty expectations and leadership reactions can also contribute to certain conduct becoming normalised, to reporting being omitted, or to the person concerned bearing the political risk of taking action.

Parties therefore have a twofold responsibility: on the one hand, to prevent and address gender-based violence and harassment within their own organisation, and on the other, to provide support to candidates, officeholders, staff and volunteers who are attacked because of their political engagement.

9.1 Zero tolerance and leadership responsibility

Every political party must state clearly and publicly that gender-based violence, sexism, sexual harassment, intimidation, stalking, gender-based online violence and retaliation cannot be regarded as an acceptable part of political competition or of the party's internal functioning.

Zero tolerance cannot be limited to a public statement. The party leadership must ensure that the rules are enforced at every level of the organisation, regardless of the political position, influence or electoral significance of the person concerned or of the perpetrator.

Leaders' responsibility extends in particular to not trivialising the cases that come to their attention, not encouraging those concerned to keep silent informally, and not allowing the protection of the party's reputation to take precedence over the safety of the person concerned or a fair investigation.

9.2 Mandatory code of conduct

Political parties should adopt a written code of conduct covering all organisational levels.

The personal scope of the code should extend to:

- the party's members and leaders;
- its elected officials;
- its candidates;
- its employees and political advisers;
- its parliamentary and local-government staff;
- its campaign teams;
- its volunteers;
- its youth and local organisations.

The rules should not apply only to conduct on the party's official premises. They should also extend to party events, conferences, travel, campaigns, electoral events, internal communication channels and the online space connected to party activity.

The code should define the prohibited forms of conduct, the reporting options, the principles of investigation, the prohibition of retaliation and the possible consequences.

9.3 Independent and confidential reporting mechanism

Parties must establish a complaint and support mechanism that all members, candidates, staff and volunteers of the party can turn to safely.

The mechanism cannot be under the exclusive control of a person who may decide on the complainant's political position, candidacy, employment or advancement.

The person concerned must also be able to request a confidential consultation before making a formal complaint, to learn about the options available, and to decide on the next steps in full knowledge of their own situation.

The mechanism must operate with clear deadlines, conflict-of-interest rules and protection against retaliation.

The internal party mechanism cannot replace police, judicial, data-protection, equal-treatment or other external remedies.

9.4 Protection against retaliation

No one may suffer political, professional or personal disadvantage for making a report or supporting a person who reports.

Retaliation may include in particular:

- removal from a candidate list or from a party office;
- withdrawal of political support;
- loss of a post or task;
- unjustified restriction of campaign resources;
- exclusion from informal decision-making;
- discrediting or threats;
- other disadvantage connected to the report.

The party's rules must treat retaliation as a separate breach of the norms, even if the investigation of the original complaint is still ongoing.

9.5 Consequences and sanctions

A standard of conduct can be regarded as a functioning institutional tool only if its breach carries institutional or disciplinary consequences that are foreseeable, transparent and adjusted to the gravity, repetition and consequences of the act.

The rules must therefore set out in advance the system of possible measures. These must take into account:

- the gravity and repetition of the conduct;
- the power differential between those involved;
- the harm caused or foreseeable;
- the risk of repetition or escalation;
- the presence of retaliation or of conduct aimed at influencing the proceedings.

The possible consequences may range from a warning and mandatory corrective measure to removal from a party or organisational office, and to further consequences permitted by the party's statutes and by applicable law.

The perpetrator's political position, elected office or electoral significance cannot serve as grounds for the absence of an investigation or for a more lenient institutional response.

9.6 Candidate selection and political advancement

Candidate selection is one of the strongest institutional tools of political parties, and it is therefore also part of preventing violence against women in politics.

In their candidate-selection and leadership-election processes, parties must make clear that gender-based violence, sexual harassment, intimidation and other serious breaches of the norms are incompatible with political leadership responsibility.

Candidates must be informed, before the campaign begins, of:

- the party's standards of conduct;
- the complaint and support mechanism;
- the digital and physical security procedures;
- protection against retaliation;
- the channels through which they can seek help.

Based on international good practice, the introduction of a candidate agreement may also be considered, in which the candidate undertakes to refrain from discriminatory, sexist and violent campaign methods and to comply with the party's standards of conduct.

The agreement must clearly set out the consequences attached to a serious breach of the rules.

9.7 Minimum campaign-period protocol

Election campaigns, candidate-selection periods and internal party leadership elections are periods of heightened risk. Greater public exposure, the intensification of online presence and the sharpening of political competition can increase the likelihood of threats, harassment and coordinated attacks.

Before the campaign begins, political parties must therefore establish a security and incident-handling protocol accessible to every candidate and campaign team.

The minimum protocol should include at least the following:

- a designated contact person available on an urgent basis;
- procedures for handling physical threats and risky events;
- minimum requirements for protecting digital accounts and personal data;
- a consistent method for documenting online attacks and threats;
- a method for securely preserving electronic evidence;
- a definition of the events that warrant escalation;
- access to legal, psychological, digital and, where necessary, physical security support;
- the possibility of maintaining contact with the police and other authorities;
- support for reporting to platforms;
- post-incident follow-up.

Particular attention must be paid to local and municipal candidates, who often have smaller teams and fewer professional resources.

The aim of the protocol is not to place the responsibility for their own protection on the candidate, but to make clear what institutional help they can expect and who is obliged to act in a dangerous situation.

9.8 Digital protection and handling of online attacks

Parties should provide regular digital-security preparation and, where necessary, expert support to their candidates and staff, particularly during election periods.

Digital protection must go beyond individual social-media usage advice. Capacity is needed for:

- recognising coordinated attacks;
- identifying serious threats;
- preserving evidence;
- maintaining contact with platforms;
- handling doxxing and manipulated content;
- where necessary, supporting official proceedings.

Parties must also take the additional workload of handling online attacks into account when planning communication and campaign capacity.

9.9 Support and the person's continued participation in politics

Parties must provide or make accessible appropriate legal, psychological, digital and security support to candidates, politicians and staff who experience violence.

The aim of support is not only to handle the specific incident. It must also extend to enabling the person concerned to continue their political activity safely, and to ensuring that the attack does not lead to unnecessary self-censorship, withdrawal or the abandonment of a political career.

Additional support may be needed where the threat also extends to family members or children, or where online and offline danger are interconnected.

9.10 Cross-party solidarity and male allies

Action against violence against women in politics gains credibility if it does not depend solely on party-political interest.

Cross-party cooperation should be supported in:

- the joint rejection of violence against women in politics;
- the sharing of good practices;
- the development of professional and supportive networks among women politicians and candidates;
- the adoption of common minimum standards;
- public solidarity in cases of serious threats and sexual harassment.

Involving male politicians and leaders is particularly important, because shaping political and organisational norms cannot be made the task of women alone. The +3R Male Pledge can be one voluntary entry point for this, but it does not replace organisational responsibility and binding internal rules.

9.11 Annual institutional self-assessment and monitoring

Political parties should assess their own functioning from the perspective of preventing and addressing gender-based political violence annually, or at least once per electoral cycle.

The self-assessment should cover at least:

- organisational and leadership culture;
- the awareness and application of the standards of conduct;
- the accessibility of reporting options;
- the handling of reports;
- protection against retaliation;
- digital and campaign security;
- the practice of candidate selection and political advancement;
- women's participation in leadership and decision-making;
- the implementation of the measures undertaken in the previous assessment.

Where possible, anonymous feedback from staff, members and candidates should also be built into the survey.

An increase in the number of reports cannot in itself be regarded as a worsening result: it may also indicate that awareness of the mechanism and trust in it have grown. In monitoring, therefore, the type, handling and outcome of cases and the experiences of those concerned must be assessed together.

On the basis of the self-assessment, the party should define concrete development tasks, responsible actors and deadlines.

Recommendations

- Every parliamentary party should adopt a code of conduct covering its entire organisation and campaign operations.
- They should establish a confidential complaint and support mechanism suitably independent of the political hierarchy.
- The rules should include an express prohibition of retaliation and foreseeable, proportionate consequences attached to breaches of the norms.
- The candidate-selection process should include acceptance of the standards of conduct and the security preparation of candidates.
- A campaign-period security and incident-handling protocol should be prepared before every election campaign.
- Parties should provide appropriate digital, legal, psychological and security support to the candidates and staff concerned.
- Cross-party women's and allies' cooperation should be supported.
- Parties should regularly assess their own functioning and attach a concrete action plan, responsible actors and deadlines to the results.

10. Institutional support and complaint mechanisms

Addressing VAWP requires an easily accessible, safe and professionally competent point of entry that the person concerned can turn to even when they do not yet know whether the case amounts to an infringement, whether they wish to make a formal complaint, or which avenue of protection is appropriate. The main problem of the current system is the fragmentation of the avenues of protection, and the lack of VAWP-specific expertise and of a unified first point of entry.

10.1 Minimum functions

The mechanism should provide:

- confidential initial contact and pre-complaint consultation;
- an initial case assessment and information on the legal, institutional and platform-level options;
- assistance in preserving evidence and, where necessary, a risk assessment;
- access to legal, psychological, digital and security support;
- the option of a formal complaint, referral and follow-up;
- anonymised data collection and the feeding back of institutional lessons.

Access to support should not be conditional on filing a formal complaint, except where the law prescribes a mandatory measure.

10.2 Independence, confidentiality and conflict of interest

The mechanism cannot be under the exclusive control of a person who may decide on the complainant's political position, candidacy, employment or advancement. Predefined conflict-of-interest rules, an alternative or external handler, adequate professional and budgetary capacity, and clear data-protection and confidentiality guarantees are needed. Independence does not necessarily mean a new institution: it can be established within an existing organisation, provided the guarantees are genuine.

10.3 A clear procedure and protection against retaliation

The procedural rules should be public and should define who is eligible, how contact is made, the deadlines, the order of hearing and decision-making, the possible measures, and the possibility of review. In urgent security situations an expedited response is required.

The complainant, witnesses and supporting persons must be protected against political, professional, employment-related or informal retaliation. Retaliation must be treated as a separate breach of the norms.

10.4 Separating support from investigation

The confidential support function and the impartial investigation cannot in every case be carried out by the same person or organisational unit. The system must ensure an appropriate separation of the support, investigation and decision-making roles, particularly in smaller political organisations.

10.5 Monitoring and evaluation

The number and type of reports, the handling time, the measures taken, the use of support services, cases of retaliation and recurring risks must be tracked regularly and in anonymised form. It must also be assessed periodically whether those concerned are aware of the mechanism, whether they consider it safe and independent, and whether the procedure reduces the burden on the person concerned.

10.6 Possible models

Three complementary models are warranted:

- a parliamentary mechanism for members and parliamentary staff;
- an internal party mechanism in line with the minimums in Chapter 9;
- an independent external advisory point, particularly for local and regional political actors.

Recommendation: Parliament and the political parties should establish a suitably independent, confidential complaint and support system protected against retaliation; in addition, the creation of a nationally accessible, party-neutral first advisory and referral point should be examined.

11. International good practices and their adaptation in Hungary

International practices do not offer a single model to follow, but adaptable operational elements. The most important lessons from the Hungarian perspective are:

Example	Working element	Adaptation in Hungary
Ireland	Treats the safety of political participation as an institutional question; candidate safety guidance, local support, police liaison	A unified safety guide, designated liaison, support for local politicians
Germany	Addressing the specific vulnerability of local political actors	An external advisory point, legal and digital-security assistance, local monitoring
OSCE/ODIHR and International IDEA	Party codes, zero tolerance, complaint mechanism, protection against retaliation, candidate support	The party-level minimums set out in Chapter 9
European parliamentary practices / UNDP-IPU	Code of conduct, confidential consultation, independent complaint-handling, sanctions, monitoring	A parliamentary standard and complaint mechanism extending also to members
IFES, electoral frameworks	The campaign as a distinct risk period; addressing online violence, gendered disinformation and AI manipulation	Pre-campaign risk assessment, rapid response, digital protection, post-election evaluation

Most elements can be launched within existing institutional frameworks. In the short term, a party code, a campaign-security protocol, digital preparation, a confidential advisory pilot and enforcement training are particularly realistic; in the medium term, a parliamentary complaint mechanism, a national advisory function, regular self-assessment and a support system for local politicians.

12. Summary recommendations and implementation framework

Implementation is built on the three pillars defined in Chapter 1: prevention, protection and response, and accountability. Measures that can be implemented in the short term can also be introduced as pilots, evaluated and further developed.

12.1 Short-term priorities

From the full system of recommendations, six priorities can be highlighted that can be started independently of, or in parallel with, legislative reform:

- Preparation and piloting of a parliamentary complaint and support mechanism.
- Introduction of minimum standards for political parties: a code of conduct, a confidential complaint mechanism, protection against retaliation and leadership responsibility.
- Development of a minimum campaign-security protocol for the physical and digital protection of candidates.

- Development of police and judicial procedural and training minimums, particularly in the areas of risk assessment, online violence and the prevention of secondary victimisation.
- A pilot of a low-threshold, independent advisory and referral function that is also accessible to local political actors.
- Development of a unified monitoring and self-assessment framework that makes it possible to track institutional change and VAWP-related experiences regularly.

The advantage of these priorities is that different actors can begin implementing them independently of one another. Political parties, for example, need not wait for legislative changes to introduce their own code of conduct, complaint mechanism or campaign-security protocol.

12.2 Implementation matrix

Responsible actor	First concrete step	Suggested timeframe	Outcome
Parliament	Development of the legal and institutional model of a conduct, complaint and support system extending to members and staff	6-12 months	Adopted rules and a functioning mechanism
Political parties	Adoption of the minimums of a code of conduct, an independent complaint channel, protection against retaliation and leadership responsibility	6 months	Public internal rules and a designated mechanism
Political parties / campaign teams	Introduction of a campaign-security protocol	before every campaign	A protocol and contact person accessible to every candidate
Police	Development of a procedural guide and risk-assessment criteria for handling VAWP and online violence	6-12 months	An applicable professional guide
Police, prosecution service, judiciary	Development of role-specific training modules	12 months	An embedded basic or continuing-training module
Government bodies responsible for legislation	Examination of the transposition of Directive (EU) 2024/1385 from a VAWP perspective	during the transposition process	A documented gap and needs assessment
Local governments and their representative bodies	A pilot survey of the security and support needs of local politicians	12 months	A pilot and an action plan
Parties, parliamentary groups, larger local governments	Introduction of annual institutional self-assessment	annually	An assessment and an action plan
Digital-security and support actors	Establishment of rapid assistance and referral for cases of serious online attacks	6-12 months	An accessible incident-handling route
Research and policy actors	Development of common monitoring indicators and data-collection minimums	12 months	Comparable annual monitoring

12.8 Monitoring and indicators

Implementation of the guidelines can be evaluated only if we define in advance what we consider progress.

It is not enough to measure only the number of incidents or reports. In the short term, an increase in reports may even be a sign of greater trust in the system.

At least four groups of indicators are therefore needed.

Institutional indicators:

- how many institutions and parties have a code of conduct;
- how many operate a complaint and support mechanism;
- how many have a campaign-security protocol;
- how many carry out regular self-assessment.

Procedural indicators:

- the number and type of reports;

- the time to first response;
- the proportion of closed cases and the duration of proceedings;
- signals relating to retaliation;
- the use of support services.

Experiential indicators:

- whether those concerned are aware of the reporting options;
- whether they consider their use safe;
- whether they trust the independence of the mechanism;
- whether they perceive an improvement in the institutional response;
- the extent to which self-censorship, withdrawal or the intention to give up a political role appears.

Participation indicators:

- the proportion of women among candidates;
- the proportion of women among elected officials;
- the proportion of women in political and party leadership positions;
- the rate of re-running and of remaining in politics, where this is measurable.

The indicators should be examined not only at national level but, where possible, also by political level, institution type and electoral period.

12.9 Annual public status review

It is recommended to produce a short, public VAWP status review each year.

This should review:

- legislative and institutional changes;
- new complaint and support mechanisms;
- the commitments of parties and political institutions;
- campaign-security measures;
- the available anonymised reporting and procedural data;
- the results of training and self-assessments;
- new forms of online violence;
- the fulfilment of the measures undertaken in the previous year.

Each annual review should be accompanied by 3-5 priorities for the coming year, together with responsible actors and deadlines.

12.10 What does success mean?

The success of the guidelines is not shown by how many new documents, codes or trainings have been created.

Change can be regarded as meaningful if:

- women in politics recognise and can safely report the violence against them;
- seeking help does not entail unpredictable political or professional risk;
- institutions respond more quickly and consistently;
- serious or escalating threats are recognised earlier;
- the burden of handling online attacks does not fall solely on the person concerned;
- breaches of the norms have foreseeable consequences;
- political leaders and witnesses take an active role;
- and attacks increasingly less often drive women to self-censorship, withdrawal or the abandonment of political participation.

The ultimate goal is not conflict-free politics. The goal is a democratic political space in which the toughness of political competition does not make gender-based violence acceptable, and in which women do not have to pay a greater personal security price for participating in public life.

Glossary

A. The phenomenon and its impacts

Violence against women in politics (VAWP).

An umbrella term for the various forms of gender-based violence and intimidation affecting women in connection with their political or public engagement. It may take psychological, physical, sexual or sexualised, economic and online forms, or a combination of these. Its aim or effect may be to restrict women's political participation, to silence them, to discredit them or to force them out of the political sphere. VAWP may affect not only elected politicians but also candidates, party members, political staff, activists and other public figures. Not every attack on a woman in politics automatically qualifies as VAWP: what is relevant to applying the concept is the gendered dimension of the attack—for example, that it targets the person because of her being a woman, or uses gender stereotypes, sexualisation, family roles or other gender-related means to weaken her political role.

Grey zone.

The range of conduct and institutional patterns that do not in every case constitute violence or an infringement in themselves, but which, appearing on a gendered, repeated or systemic basis, can contribute to restricting women's political participation. This may include, for example, regular sexist remarks, the consistent devaluation of professional performance, exclusion from informal decision-making, or other treatment based on gender stereotypes. The purpose of the concept is not to classify every unpleasant political interaction as violence, but to recognise recurring patterns.

Normalisation.

The process by which gender-based attacks or problematic conduct gradually come to be seen as a natural or inevitable feature of political life. A typical form is the trivialisation of cases with arguments such as "it's part of politics", "a public figure has to put up with this" or "it was just a joke".

Online violence.

An umbrella term for threatening, harassing, intimidating, sexualised or other harmful conduct carried out using digital technologies or online platforms. This may include, for example, online threats, cyberstalking, coordinated harassment, the malicious disclosure of personal data, and the dissemination of intimate or manipulated content. The legal assessment of individual acts may differ. Online and offline violence can be interconnected.

Cyberstalking (online threatening surveillance).

Repeated or continuous following, surveillance or contact carried out by digital means that may cause the person concerned fear or a security risk. Together with other threatening conduct, online surveillance can also escalate into a physical security risk.

Doxxing.

The disclosure, with harmful or intimidating intent, of personal data or of information enabling the identification, contacting or physical location of the person concerned. The publication of information about a home address, contact details, family members, children or regularly visited places can be particularly risky. Not all disclosure of personal data is unlawful, so the legal assessment always depends on the circumstances of the case.

Coordinated online attack.

A pattern of online attack in which several users, pages, accounts or communication channels target a person within a short time in a coordinated or mutually reinforcing manner. The fact of coordination cannot always be proven, so in institutional assessment the volume, timing, repetition and pattern of the attack must be examined together.

Gendered disinformation.

The dissemination of false, manipulated or misleadingly contextualised information that draws on gender stereotypes, sexualisation, private life or prejudices about women's social role in order to discredit the person concerned or weaken their political participation.

Hypervigilance (heightened alertness).

The continuous heightened attention and security readiness associated with sustained or repeated exposure to threat. In the case of women in politics it may appear, for example, in the constant monitoring of online spaces, the physical environment, the safety of family members or possible attacks. It can cause a significant psychological and work burden.

Reporting gap.

The difference between the number of violent or harassing incidents actually experienced and the number of officially reported cases. A large reporting gap may be due to several factors, such as a lack of trust in the procedure, fear of retaliation, unfamiliarity with the available mechanisms, the normalisation of the case, or previous negative experiences. A low number of reports therefore does not in itself prove a low incidence.

Secondary victimisation.

The further harm or burden that the person concerned experiences not directly from the original attack, but as a result of the institutional, official or social reaction to it. This may include victim-blaming, unnecessarily repeated hearings, trivialisation or an unjustified procedural burden.

Retaliation.

A disadvantage suffered by a complainant, witness or person supporting the person concerned in connection with the report or their involvement. In a political environment it may appear, for example, as the loss of a candidacy or office, the withdrawal of political support or resources, exclusion from informal decision-making, discrediting or threats.

Chilling effect on political participation.

A consequence of an attack or of institutional conduct that affects whether the person concerned speaks up, which issues they take on, whether they run in an election, whether they take on a leadership role, and whether they continue their political or public activity. The effect may be direct or gradual, and may appear as self-censorship, withdrawal or the abandonment of a political role.

B. Institutional and preventive tools

Risk assessment.

A structured examination of the circumstances of a case to determine whether there is a risk of repetition, escalation or physical danger, and what protective measures are needed. It is particularly important in cases of repeated threats, stalking, doxxing, the acquisition of information about a person's physical whereabouts, and threats against family members or children.

Pattern-based assessment.

An approach that examines individual incidents not only in isolation but together with their antecedents, their repetition, their relationship to one another and their possible escalation. It is particularly relevant in cases of online harassment, stalking, threats and attacks across several communication channels.

Independent complaint and support mechanism.

An institutional or external system that the person concerned can turn to safely for advice, support or to make a formal complaint, and which operates with appropriate guarantees of independence, confidentiality and freedom from conflicts of interest. The support and investigation functions of the mechanism must be separated where necessary.

Confidential preliminary consultation.

A low-threshold option through which the person concerned may, before filing a formal complaint, seek information about their options, the likely course of the procedure, the forms of support and any risks. The consultation does not in itself automatically initiate a formal procedure, except where the law prescribes a mandatory measure.

Campaign-security protocol.

An institutional set of procedures established before an election campaign that defines the physical and digital security minimums, the documentation of threats, risk assessment, the possibility of rapid escalation, the contact persons, and the available legal, psychological, digital or security support.

Institutional self-assessment.

A regular, structured examination by a political or public institution of its own functioning from the perspective of VAWP risks and institutional protection. It may examine, among other things, organisational culture, leadership reactions, complaint mechanisms, the risk of retaliation, digital and campaign security, and women's participation in decision-making.

Gender audit.

A structured assessment method that examines how an organisation's rules, resources, decision-making processes, operating culture and outcomes affect different genders, and where structural inequalities can be identified.

Leadership responsibility.

The responsibility of political or institutional leaders for ensuring that clear standards of conduct, safe complaint and support options, an appropriate response and accountability operate in their organisation. It includes avoiding the

trivialisation and concealment of problematic conduct, and ensuring that the protection of the organisation's reputation does not override the safety of the person concerned or a fair procedure.

Intersectionality (intersecting disadvantages).

The recognition that gender-based disadvantages, combined with other social circumstances and prejudices, can result in different or heightened exposure. Such factors may include, for example, age, disability, ethnic or national background, migrant status or geographic location.

Male Pledge (Declaration of Democratic Commitment).

A voluntary pledge tool developed within the +3R project that encourages primarily male political and public actors to reject gender-based political violence, to show solidarity and to support institutional change. It does not replace binding codes of conduct, complaint mechanisms or institutional responsibility.

C. Legal and policy frameworks

VAW Directive (Directive (EU) 2024/1385).

The Directive of the European Parliament and of the Council on combating violence against women and domestic violence. It provides, among other things, for the criminalisation of certain forms of online violence, the support and protection of victims, reporting options and official capacities. The deadline for Member State transposition is 14 June 2027.

Istanbul Convention.

The Council of Europe Convention on preventing and combating violence against women and domestic violence (CETS No. 210). It emphasises four interconnected areas: prevention, protection and support, prosecution, and coordinated policy action. Hungary signed it in 2014 but has not ratified it. In these guidelines it also serves as a policy benchmark.

CEDAW.

The UN Convention on the Elimination of All Forms of Discrimination against Women. Its obligations relating to women's political and public participation, to state action against gender-based violence and to the elimination of structural inequalities are also relevant to VAWP.

DSA (Digital Services Act).

Regulation (EU) 2022/2065 on digital services. It sets out rules on, among other things, the operation of online intermediary services and platforms, the reporting of illegal content, transparency and the systemic risk management of certain providers. It does not create a separate VAWP category, and does not automatically render all sexist or offensive content unlawful.