Promo-LEX
Advancing democracy and human rights

RESEARCH REPORT

PROTECTION OF PERSONAL DATA IN THE ELECTORAL PROCESSES OF THE REPUBLIC OF MOLDOVA

Chisinau, 2026

Authors:
Mrs. Tetyana BOHDANOVA, expert in personal data protection and electoral processes
Mr. Sergiu BOZIAN, expert in personal data protection

Graphic design and layout: Marina Bejenari

DISTRIBUTED FREE OF CHARGE

This report has been produced within the framework of the project "Democracy in Action: Strengthening Electoral Integrity, Political Accountability, and Civic Participation," implemented by the Promo-LEX Association, with the support of the Government of the United Kingdom of Great Britain and Northern Ireland and Sweden.

Table of Contents

I. Abbreviations

CEC – Central Electoral Commission

CNPDCP – National Center for Personal Data Protection (Centrul Naţional pentru Protecţia Datelor cu Caracter Personal al Republica Moldova)

IDNP – Personal numerical code assigned by the state to an individual

RSA – State Register of Voters (Registrul de Stat al Alegatorilor)

SAISE – State Automated Information System "Elections"

GDPR – General Data Protection Regulation (EU) 2016/679

DPO – Data Protection Officer

DPIA – Data Protection Impact Assessment

II. Key Terminology

Personal data – Any information that identifies or may lead to the identification of a natural person (**personal data subject**), including but not limited to: name, surname, home address, telephone number, date/month/year of birth, profession/position, banking details, and data regarding financial status.

Personal data operator – A natural or legal person, of public or private law, who determines the purposes of processing personal data and, where appropriate, the means used.

Processing of personal data – Any operation or set of operations performed on personal data or on sets of personal data, with or without the use of automated means, such as:

- **Collection** – Gathering, accumulating or receiving personal data by any means and from any source.
- **Storage** – Keeping the collected personal data on any kind of medium (paper and/or electronic format), including by making backup copies.
- **Use** – The use of personal data, in whole or in part, by and within the operator, the operator's agents or the recipient, including by printing, copying, duplicating, scanning or other similar processes.
- **Disclosure/Dissemination** – Making personal data available to third parties by communication, transmission, dissemination or making it available in any other way.
- **Deletion** – The elimination or removal, in whole or in part, of personal data from records or recordings, by fulfilling the retention period, upon achieving the purpose for which they were entered, obsolescence, non-existence, or inaccuracy.

Depersonalization of data – Modification of personal data so that details regarding personal or material circumstances no longer allow their attribution to an identified or identifiable natural person, or allow attribution only under conditions requiring disproportionate expenditure of time, means and manpower.

Pseudonymization of data – The processing of personal data in such a way that it can no longer be attributed to a specific data subject without the use of additional information, provided that this additional information is stored separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Rights of personal data subjects – The rights provided for in art. 12-17 of Law no. 133/2011 on the protection of personal data: the right to be informed, to have access to data, to intervene, to oppose, and not to be subject to an automated decision.

Means of processing personal data – The methods of collection, storage, use, disclosure, dissemination, joining, combining, destruction, etc., applied to personal data, including the software (applications/programs) and hardware (computer, server or any other device) used.

Data Protection Officer (DPO) – A person appointed internally or externally according to art. 25 of Law no. 133/2011 or art. 37 of Law no. 195/2024 and who possesses the necessary qualities and completeness according to art. 25/1-25/2 of Law no. 133/2011 or art. 38-39 of Law no. 195/2024

Personal Data Protection Impact Assessment (DPIA) – A mandatory verification process according to the requirements of article 23 of Law no. 133/2011 or art. 35 of Law no. 195/2024 when one or more data processing operations generate or are likely to generate a high risk to the rights and freedoms of data subjects.

III. Executive Summary

This report examines the personal data protection practices of key actors in Moldova's electoral ecosystem – nine parliamentary political parties, the Central Election Commission (CEC), and the National Centre for Personal Data Protection (CNPDCP) – against the backdrop of the 2024-2025 electoral cycles and the approaching transition to Law No. 195/2024, which aligns Moldovan law fully with the GDPR and enters into full force on 23 August 2026.

Moldova's electoral ecosystem faces threats of documented severity – including the mass cross-border transfer of voters' personal data to the Russian Federation for the purposes of voter bribery, fictitious pre-registrations affecting thousands of citizens across two consecutive electoral cycles, and the exploitation of personal data in alleged foreign influence operations. These incidents represent documented, ongoing risks to electoral integrity with direct consequences for democratic participation.

Against this threat environment, institutional readiness is found to be critically insufficient across all three actors assessed. Among parliamentary parties, four of nine did not respond to formal information requests. Of the remaining parties, officials demonstrated limited understanding of what constitutes personal data processing and which operations their own parties are conducting – whether in a digital realm or offline. Website analysis revealed near-universal absence of compliant cookie notices, inadequate or missing privacy policies, unverified donation forms, and cross-border data transfers – including to jurisdictions without adequate data protection frameworks. Further analysis confirmed that parties struggle when it comes to complying even with the key data protection obligations, such as developing internal data protection policies (only one has provided a more comprehensive policy for analysis, while three shared a link to privacy policies on their websites), appointing a Data Protection Officer (three) and notifying the CNPDCP (none); only two of five responding parties reported conducting a Data Protection Impact Assessment.

The CEC demonstrates greater institutional awareness and several areas of good practice, including adopting measures that restrict access to the State Register of Voters and depersonalization of published correspondence. However, it has not conducted a DPIA for any of its major data processing systems – despite a legal obligation in force since 2022, and its data protection policy references repealed legislation.

The CNPDCP has largely operated reactively. In the past five years, it conducted no self-initiated controls in the electoral domain, issued no updated guidance for electoral actors since 2013, and provided no training to parties or the CEC. Its own website employs a non-dismissible cookie banner and references regulatory acts that have been repealed.

The transition deadline of 23 August 2026 represents a narrowing but defined window for reform. The report sets out detailed recommendations for each actor, prioritizing DPIA completion, substantive DPO designation, privacy policy compliance, cessation of high-risk third-party data transfers, and proactive enforcement by the CNPDCP – including sector-specific guidance and targeted controls ahead of the next electoral cycle.

IV. Research Objectives and Methodology

1. Focus and scope of the study

This report examines the personal data protection practices of the principal actors in Moldova's electoral ecosystem – nine Parliamentary political parties: Partidul Acțiune și Solidaritate (PAS)/Party of Action and Solidarity, Partidul Socialiștilor din Republica Moldova (PSRM)/Party of Socialists of the Republic of Moldova, Partidul Nostru/Our Party, Partidul Democrația Acasă (PDA)/Democracy at Home Party, Partidul Comunistilor din Republica Moldova (PCRM)/Party of Communists of the Republic of Moldova, Partidul „Mișcarea Alternativa Națională"/National Alternative Movement Party, Partidul Dezvoltării și Consolidării Moldovei (PDCM)/Party for the Development and Consolidation of Moldova, Congresul Civic/Civic Congress, Partidul Viitorul Moldovei (PVM)/Future of Moldova Party, the Central Election Commission (CEC), and the National Centre for Personal Data Protection (CNPDCP) – against the backdrop of the 2024-2025 electoral cycles, which encompassed presidential elections, a constitutional referendum, and parliamentary elections.

The study is shaped by a critical legislative transition: the adoption of Law No. 195/2024 on Personal Data Protection, which fully aligns Moldovan law with the EU General Data Protection Regulation (GDPR) and enters into binding force on 23 August 2026. This transition window defines the reform horizon against which institutional readiness is assessed.

The report pursues three interrelated objectives. First, it documents the threat environment: incidents during 2024-2025 involving documented misuse of voter data, including mass cross-border transfers to the Russian Federation for voter bribery and fictitious pre-registrations affecting tens of thousands of citizens. Second, it assesses current data protection practices of the two actors against the requirements of Law No. 133/2011, with reference to the approaching obligations of Law No. 195/2024, identifying compliance gaps and risks to voters' rights. Third, it evaluates the CNPDCP's effectiveness as a regulator in the electoral domain.

The scope of the study is deliberately bounded. It does not purport to offer a comprehensive audit of any single institution, and while its intention is not to reach definitive legal determinations on the lawfulness of specific processing operations, the study does point out obvious gaps in compliance and practices contradictory to the current legal framework. In addition, it strives to provide a structured, expert assessment of observable practices and known incidents, designed to inform policy dialogue and practical reform efforts among political actors, electoral management bodies, the data protection authority, and Moldovan civil society.

2. Methodological approach

The research combines four principal lines of inquiry, each targeting a distinct actor or category of incidents within the electoral data protection landscape. Together, they form an integrated methodology that triangulates findings across institutional types, data collection modes, and analytical frameworks. The approach draws heavily on the international methodology developed by the National Democratic Institute (NDI), with input from an expert advisory group convened in 2025 for the purpose of producing standards and tools for the assessment of personal data practices in electoral contexts.

The assessment was carried out between December 2025 and March 2026 by two subject-matter experts – an international data protection and elections researcher Tetyana Bohdanova and a domestic legal expert with extensive expertise in Moldovan data protection law and its application Sergiu Bozianu – at the request of and in close cooperation with Promo-LEX Association. The combination of international comparative expertise, domestic legal knowledge, and in-country electoral observation and analytical experience is essential to producing findings that are both technically grounded and contextually credible.

2.1 Desk research

The first line of inquiry focuses on documented or credibly alleged incidents involving the potential misuse of voters' personal data during the 2024-2025 electoral cycles – a period characterised by a heightened threat environment, with documented disinformation campaigns, allegations of foreign interference, and concerns about voter data acquired through irregular channels.

Sources reviewed include decisions and reports from the CEC, the CNPDCP, and law enforcement authorities (including that of Security and Intelligence Service of the Republic of Moldova), media publications, and election observation reports of the Promo-LEX Association. This information was supplemented by the data obtained from interviews and questionnaires distributed to the political parties, the CEC, and the CNPDCP. Reviewed incidents were selected on the basis of their relevance to personal data processing, covering targeted campaign communications, data processing for election administration purposes, and the exploitation of personal data in support of alleged influence operations.

Additional desk research informed the research team's understanding of the general use of personal voter data in Moldovan elections, its legal and electoral framework, and the state of personal data protection regulations in Moldova.

2.2 Assessing parliamentary political parties

The second line of inquiry examines the personal data processing practices of Moldovan parliamentary political parties – that is, parties represented in the Parliament of the Republic of Moldova as constituted following the September 2025 parliamentary elections. Political parties are among the most consequential data controllers in the electoral ecosystem: they collect, analyse, and act upon personal information about voters at scale, across a diverse range of channels, and with significant variation in technical sophistication and institutional capacity. The assessment of party practices is accordingly the most methodologically varied component of the study.

- **Website Analysis**: Each parliamentary party's official website was examined using a structured analytical framework derived from the requirements of Law No. 133/2011 (while taking into account Law No. 195/2024) and Law no. 284/2004 on information society services, where relevant. The review assessed the presence and adequacy of privacy notices and cookie policies; the lawfulness and transparency of consent mechanisms for data collection through web forms, newsletter subscriptions, volunteer registration, or donation functionality; and the use of tracking technologies including cookies, pixels, and analytics scripts; the presence of links to third-party platforms and the associated data-sharing implications; and the accessibility and completeness of data subject rights information. Website analysis was conducted by the research team between mid-January and early March 2026 and any findings do not reflect the change of content or settings that may have occurred after this period. To analyze the use of cookies, trackers, or other analytical scripts, the team used Blacklight, a realtime website privacy inspector built by a nonprofit newsroom The Markup. All analysed websites are listed in **Annex 2**. The research team has not analyzed the online activity of the parties on social networks, given an extended period of time since the elections.
- **Official requests for information:** in February 2026 Promo-LEX Association submitted official requests for information to all abovementioned parties. The requests for information included a structured questionnaire and a request for an interview. The questionnaire sought information on: the types of personal data collected and the purposes for which they are processed; the legal bases relied upon for processing operations, including the processing of special categories of data such as political opinions; the use of data analytics, profiling, or micro-targeting tools in campaign activities; third-party data sharing arrangements, including with digital campaign service providers inside or outside Moldova; the implementation of data subject rights procedures; the existence and content of internal data protection policies; and other. The full questionnaire is reproduced in **Annex 3**. Out of **nine** Parliamentary political parties that had been sent the request, **four**[1] failed to provide a response, including: Partidul Democrația Acasă (PDA)/Democracy at Home Party, Partidul Comunistilor din Republica Moldova (PCRM)/Party

[1] Partidul Viitorul Moldovei/Future of Moldova Party provided responses to the questionnaire during an interview.

of Communists of the Republic of Moldova, Partidul „Mișcarea Alternativa Națională”/National Alternative Movement Party, and Congresul Civic/Civic Congress.

- **Interviews:** Semi-structured interviews were conducted in a hybrid format with representatives of **five** parliamentary parties, including party officials with senior leadership roles in the party and/or legal and compliance functions, during the period of February 24-March 6, 2026. Most interviews were conducted jointly by a domestic and an international expert. Interviews built on the responses received for the questionnaire and were meant to elicit more detailed and contextual information than the structured questionnaire permits, and to explore specific practices, challenges, and institutional attitudes towards data protection compliance in greater depth. All interviews were conducted on a named basis unless a participant(s) specifically requested otherwise. It was not possible to conduct the interview with the four political parties that did not respond to the request for information, as well as with the Partidul Acțiune și Solidaritate (PAS)/Party of Action and Solidarity (within the period of the given research).

2.3 Assessing the Central Election Commission

The third line of inquiry examines the personal data processing practices of the Central Election Commission (CEC), the principal electoral management body responsible for the conduct of national elections in the Republic of Moldova. The assessment was conducted through a **structured questionnaire** – reproduced in full in **Annex 4** – submitted to the CEC, supplemented by a **semi-structured interview** conducted online. Notably, the CEC provided the response within two calendar days of receiving the official request for information and followed up with additional requested materials, as well as promptly agreed to an interview.[2]

The questionnaire focused on four thematic areas: the CEC's internal data protection governance structures, including the appointment of a data protection officer (DPO), adoption of internal policies, conducting the personal data protection impact assessment (DPIA), and engagement with the CNPDCP; the management of the State Register of Voters (RSA); the handling of candidate registration and party finance disclosures, with particular attention to the boundary between publicly available and access-restricted personal data; and the data protection implications of video surveillance at polling stations. The findings drawn from the questionnaire responses, the interview, and additional provided materials are integrated throughout Chapter V. Key Findings, Section 3. Central Election Commission.

2.4 Evaluating the activity of the National Center for Personal Data Protection

The fourth line of inquiry examines the practices and supervisory posture of the National Centre for Personal Data Protection of the Republic of Moldova (CNPDCP), the authority responsible for enforcing data protection law and promoting compliance across all sectors, including the electoral domain. The assessment was conducted through a **structured questionnaire** – reproduced in full in **Annex 5** – submitted to the CNPDCP Director. Notably, the CNPDCP attended an interview four days after the legally mandated deadline[3] and provided a written response even later, which fell outside of the period of this analysis. The research team has also reviewed the CNPDCP website.

The questionnaire focused on three interrelated dimensions of the CNPDCP's regulatory activity in the electoral field: 1) its enforcement and supervisory record, including the number and handling of complaints filed against political parties and the CEC, self-initiated controls, and any cases involving non-compliant cross-border transfers of voter or party member data; 2) its capacity-building and outreach activities, including the issuance of sector-specific guidance or instructions, training conducted with parties and the CEC, and the rate of data protection officer appointment notifications by electoral actors; 3) and its institutional readiness and self-assessment, including the volume of prior consultation requests received from parties and the CEC, use of its power to prohibit the processing of special categories of data, steps taken to promote compliance in the electoral domain,

[2] In accordance with the provisions of Law No. 148/2023 on access to information of public interest, political parties, the CEC and CNPDCP are information providers (art. 5). The deadline for examining the request for access to information is up to 10 calendar days (art. 19 para. (1)) and the method of obtaining the information is determined by the applicant (art. 20 paragraph (1)).
[3] ibid.

initiatives to strengthen the legislative framework, and its own assessment of the adequacy of existing legal tools and the overall state of personal data processing in electoral contexts. The findings drawn from interview responses and the review of the CNPDCP website are integrated throughout Chapter V. Key Findings, Section 4. National Center for Personal Data Protection.

3. Normative framework for the assessment

The assessment is conducted against a defined normative framework anchored in the Law No. 133/2011, but takes into account the requirements of Law No. 195/2024 on Personal Data Protection which was published in the official gazette on 25 July 2024 and is set to become fully binding on 23 August 2026.

The evaluative criteria applied across assessments of political parties and the CEC includes: the lawfulness of processing and the identification of appropriate legal bases, including for special categories of data such as political opinions; compliance with the principles of purpose limitation, data minimisation, accuracy, and storage limitation; transparency obligations and the adequacy of privacy notices; the existence of consent mechanisms and data subject rights procedures; institutional governance measures, including the appointment of data protection officers, the conduct of data protection impact assessments, and the implementation of technical and organisational security measures; the handling of third-party data sharing, cross-border transfers, and direct marketing communications. In the case of the CNPDCP, the analysis reviews adequacy of supervisory tools and enforcement activity. The applicable regulations are discussed in more detail in **Annex 1.**

4. Limitations

The findings of this report reflect the state of personal data processing practices as documented primarily after the conclusion of the 2024-2025 electoral cycles. The analysis of political parties' websites and online data collection mechanisms was conducted during January-March 2026, and the requests for information and interview letters were submitted to the CEC and CNPDCP in February 2026. This timing means *the report captures a post-electoral snapshot of the online activity rather than a real-time account of practices as they operated during the campaigns themselves*. Website functionality, tracking configurations, and data collection mechanisms may have changed between the electoral period and the point of analysis – and, indeed, may change again after it.

The completeness of the assessment is further constrained by the responsiveness of the actors surveyed. As mentioned above, only **five** parliamentary parties responded to the structured questionnaire, and only **four** of them agreed to participate in interviews, limiting the depth of findings for those parties and increasing the relative weight placed on external website analysis and desktop research. Where no response was received, this is noted in the relevant findings section and treated as a data point in its own right. Furthermore, for both questionnaires and interviews, *findings are limited to what respondents chose to disclose to the research team*, with limited possibility to verify responses. Similarly, the information obtained from the CEC and the CNPDCP reflects what those institutions *chose to disclose* in the context of a requested information exchange, rather than the product of a formal audit with compulsory disclosure powers.

Importantly, the research covered key aspects accessible for the study, but *cannot claim that the conclusions and gaps found are exhaustive*, as the research team did not have access to registers, databases, buildings, and the infrastructure used, nor conducted a thorough evaluation of every aspect of processing personal data in the electoral context.

These constraints do not undermine the overall findings but mean the report should be read as a structured expert assessment based on available evidence, rather than an exhaustive institutional audit.

V. Key Findings

1. Background: recorded incidents involving the misuse of voter personal data in the 2024-2025 electoral cycles

The research team examined documented incidents of voter personal data misuse during the 2024 Presidential election and Constitutional referendum and the 2025 Parliamentary elections – a period marked by disinformation campaigns, foreign interference allegations, and concerns about irregularly obtained voter data – to build an empirical foundation for the assessment. Sources included decisions and reports from the CEC, CNPDCP, Moldova's Security and Intelligence Service (SIS), media publications, and Promo-LEX election observation reports. The analysis was supplemented by interviews with and questionnaires received from the political parties, the CEC, and the CNPDCP. Incidents were selected for their relevance to personal data processing, covering areas such as targeted campaign communications, commercial acquisition of voter data, data breaches, and exploitation of personal data in alleged influence operations.

The most grave recorded incidents involved the collection and transfer of personal data abroad for the purpose of voter bribery or fraudulent registration for voting.

Thus, during the 2024 Presidential Elections and Constitutional Referendum, Promo-LEX field observers reported mass collection and transfer to the Russian Federation voters' personal data – in particular, through the use of a popular messenger Telegram's chatbot functionality[4] – which collected personal data of voters from their identity documents and their bank account numbers in return for a small payment, for the purposes of citizen mobilization with promises of more payouts. Observers also reported other instances of the same political force attempting to collect data from voters' identification documents in exchange for cash. Reviewed media publications further note that actors investigated in 2025 for illicitly collecting citizens' data and transferring it to the Russian Federation have also utilized a mobile application disseminated via Telegram[5]. This information was supplemented by an unclassified SIS report[6], which shed light on the scale of the operation, noting that it may have reached approximately 84,000 voters. The report states that the scheme involved opening bank accounts for Moldovan citizens in the Russian *Promsvyazbank* for the purpose of large-scale voter bribery.

Notably, in these cases, Moldovan citizens' personal data has been transferred to a jurisdiction that, according to art. 32 of Law no. 133/2011 and the CNPDCP Decision no. 33/2022 on the approval of the list of states that ensure an adequate level of protection of personal data, does not ensure such adequate level of protection. Furthermore, in the absence of relevant data protection agreements with the Russian Federation, Moldovan national authorities lack effective jurisdiction to investigate or sanction violations occurring on Russian territory once data has been transferred.

Following such incidents, the CNPDCP has used its website and social media channels to advise voters to be more cautious when providing their personal data. However, according to the interview with the CNPDCP representatives, no special media coverage (beyond reporting related to the investigations of the Şor network) was given to this issue that could help raise voter awareness about data protection. The team conducted a search on the CNPDCP website and was able to identify very few relevant publications; moreover, the reference date on the publications has not always been included.[7]

[4] In September 2024, Ilan Şor, leader of BP Victorie, alleged enrollment of over 800,000 persons via the chatbot functionality on his Telegram channel. See MISIUNEA DE OBSERVARE ALEGERI PREZIDENȚIALE ȘI REFERENDUM CONSTITUȚIONAL 20 OCTOMBRIE (3 NOIEMBRIE) 2024 (RO) for more details.

[5] https://newsmaker.md/ru/video-mobilnoe-prilojenie-dlya-podkupa-izbiratelei-na-predstoyashih-vyborah-podrobnosti-obyskov-po-delu-gruppy-shora (RU).

[6] FRAUDELE ELECTORALE CONSTATATE ÎN CADRUL ALEGERILOR PREZIDENȚIALE ȘI A REFERENDUMULUI REPUBLICAN: Imixtiunea externă în procesele electorale din Republica Moldova (RO).

[7] For the list of identified publications, see Chapter V. Key Findings, Section 4. National Center for Personal Data Protection.

Despite the heightened risk of voter data abuse demonstrated by such incidents, the CNPDCP has played a rather reactive role in the electoral process since. According to the abovementioned interview – while it responded to the complaints from the CEC, the data subjects, or the information from the law enforcement authorities – the Center has not taken any special or proactive measures in this regard; such as, for example, initiating the review of data processing practices of other political forces that have run in the 2024 Presidential or the subsequent 2025 Parliamentary elections, issuing dedicated guidelines for the CEC, candidates, or political parties on personal data processing during elections, or conducting additional awareness-raising activities for the voters (e.g., in the media).

Moreover, pursuant to Article 27 of Law No. 133/2011 on the protection of personal data, the CNPDCP examines complaints within a period of three months, with the possibility of extension up to six months – which is a very long period given the urgent nature of the examined electoral threats and the interventions needed by the CNPDCP and other competent authorities to promptly identify and effectively sanction those responsible, also to prevent further violations.[8] (For more information on the activities of the CNPDCP and relevant recommendations, see Chapter V. Key Findings, Section 4. National Center for Personal Data Protection and Chapter VI. Conclusions and Recommendations).

Another critical incident involved massive preliminary voter registrations for out-of-country voting (on the territory of the Russian Federation), which reached 8,238 cases in 2024 – approximately eight times the 2021 figure – despite a documented decrease in the number of Moldovan citizens residing in Russia.[9] In the interview, the CEC representatives stated that it was established that "someone had massively registered persons for polling stations in the Russian Federation, while those persons were actually in the Republic of Moldova" (own translation of the CEC quote by the research team). Moreover, the practice has continued into 2025, with the CEC confirming during the interview that approximately 13,000 registrations were identified in connection with the parliamentary elections. Media reports provided further evidence of registrations being submitted on behalf of Moldovan citizens residing in Moldova without their knowledge.[10] Investigations into both incidents failed to identify the perpetrators, as the CEC stated they could not be traced by foreign-based IP addresses. Notably, these incidents indicate that another mass cross-border transfer of citizen data may have taken place to a jurisdiction lacking adequate level of protection of personal data.

Already in 2024, the election observers have drawn the attention of the CEC to the fact that the pre-registration procedure is extremely easy and only requires passport data to submit an application. Simply put, there are no certain mechanisms to validate the identity of the person and to exclude an abusive registration of this data, such as: an electronic signature, other trusted means, etc. Moreover, such “pre-registered” voters are then removed from the voter lists at their main polling stations, which further complicates voting for those whose data had been misused in such a manner.

Additionally, in the event of detection of such security incidents in the processing of personal data, data subjects are not informed that their personal data have been subject to non-compliant processing, in order to pave the way for the defense of their rights in civil, administrative, contravention or criminal proceedings.

Following the 2024 instance of fraudulent voter pre-registration, Promo-LEX has already recommended that a data protection impact assessment is conducted for the State Automated Information System "Elections" (SAISE). However, since this obligation has existed since 2022[11] – according to the findings of this study – no DPIA has been conducted by the CEC. (For more information on the activities of the CEC and relevant recommendations, see Chapter V. Key Findings, Section 3. Central Election Commission and Chapter VI. Conclusions and Recommendations).

[8] The Law no. 195/2024 extends this period even further, setting the period for conducting the investigation to up to 6 months from the date of initiation of the investigation, with the possibility of a justified extension by one month, but not more than 12 months from the date of its initiation, depending on the complexity of the case, the volume of information to be obtained and examined, the behavior of the participants in the investigation procedure, and other relevant aspects (art. 81 par. (25) of Law no. 195/2024).

[9] See the PRESIDENTIAL ELECTIONS AND REPUBLICAN CONSTITUTIONAL REFERENDUM OCTOBER 20, 2024: Report No. 2 (EN) for more details.

[10] https://gagauzinfo.md/index.php/news/politics/vi-chto-tam-mutite-dodon-uznal-chto-zaregistrirovalsya-dlya-golosovaniya (RU).

[11] The need to carry out a data protection impact assessment is established starting with 2022 by Law no. 175/2021 (the obligation being introduced in art. 23 of Law no. 133/2011).

Notably, the repeat nature of some of these incidents does not allow excluding the possibility of the voter data illicitly collected and processed in 2024-2025 being abused during the future electoral cycles by the same actors – unless necessary preventive measures are taken.

2. Political parties

2.1. Political Parties' Websites: What we observed

Overview

The research team analysed the official websites of all **nine** parliamentary political parties represented in the Parliament of the Republic of Moldova following the September 2025 elections. The full list of analysed websites is reproduced in **Annex 2**. Each website was examined in the period of January-February 2026 using a structured framework that assessed four elements: the presence and operation of third-party tracking technologies, as detected using the Blacklight real-time privacy inspector; the types of data collection forms and interactive functionalities offered; the existence, content, and legal adequacy of privacy policies, cookie notices, and terms and conditions; and compliance with the specific requirements of Articles 12 and 25 of Law No. 133/2011 on Personal Data Protection and Article 10(2) of Law No. 284/2004 on Information Society Services – the provisions governing transparency, privacy notices, and consent that remain applicable during the transitional period preceding full entry into force of Law No. 195/2024.

The website review was conducted from two single external access points (one from inside and one from outside Moldova) at a defined moment in time, without back-end access to parties' platforms or systems. The functionality encountered may differ from that experienced by users accessing the same sites from different devices, browsers, or IP addresses, meaning the analysis represents a necessarily partial and time-bound picture of each party's online data processing environment.

Widespread Shortcomings

The website analysis revealed a set of compliance deficiencies that are systemic across the parliamentary party landscape rather than isolated to individual actors.

- **Absence of cookie notices:** The most pervasive shortcoming is the absence of compliant cookie banners and consent mechanisms: the majority of parties deploy third-party tracking scripts – most frequently from Alphabet Inc. (Google Analytics) – while **none** notify users or offer any mechanism to accept or refuse cookies.
- **Shortcomings in the privacy policies: four** of the **nine** analysed websites did not seem to have a privacy policy or display data protection notices at all at the time of analysis, including socialistii.md (PSRM), partidulnostru.md (Partidul Nostru/Our Party), pcrm.md (PCRM), and congresulcivic.md (Congresul Civic/Civic Congress). The remaining **five** websites – unpaspentru.md (PAS), pda.md (PDA), alternativa.eu (National Alternative Movement PartyPartidul „Mișcarea Alternativa Națională"/National Alternative Movement Party), pdcm.md (PDCM), and viitorulmoldovei.md (PVM) – have published privacy policies. However, they are in most cases formal documents that fail to meet the minimum transparency requirements of the law: they do not identify the data controller and authorised processors, do not specify the categories of personal data processed, their purposes, or their legal bases, and do not indicate storage periods, data subject rights, or the contact details of a data protection officer.
- **Cross-border data transfers, including to jurisdictions without an adequate data protection framework**: as of January 2026, **all** of the assessed parties appear to carry out some cross-border data transfers via their websites – in some cases to servers located outside Moldova and the EU – i.e., through the use of Gmail addresses for parties' official contacts, digital services platforms, such as Cloudflare, audience analysis scripts and trackers by social media companies such as Google Analytics and Yandex Metrics, mostly without any indication that appropriate safeguards are in place.

- **Improper identity verification for donations:**[12] Donation forms across **five** of the **nine** websites lack identity verification mechanisms, raising concerns about both data integrity and the security of financial processing. Including: congresulcivic.md (Congresul Civic/Civic Congress), pdcm.md (PDCM), alternativa.eu (Partidul „Mișcarea Alternativa Națională”/National Alternative Movement Party), pda.md (PDA), and unpaspentru.md (PAS).
- **Misunderstanding consent: three** of the **nine** analysed websites, including unpaspentru.md (PAS), pda.md (PDA), and pdcm.md (PDCM) erroneously cite consent as the legal basis for processing in contexts where it is either inapplicable or improperly obtained – a recurring misunderstanding of the legal framework that the analysis documents across parties of varying political orientation and institutional capacity.

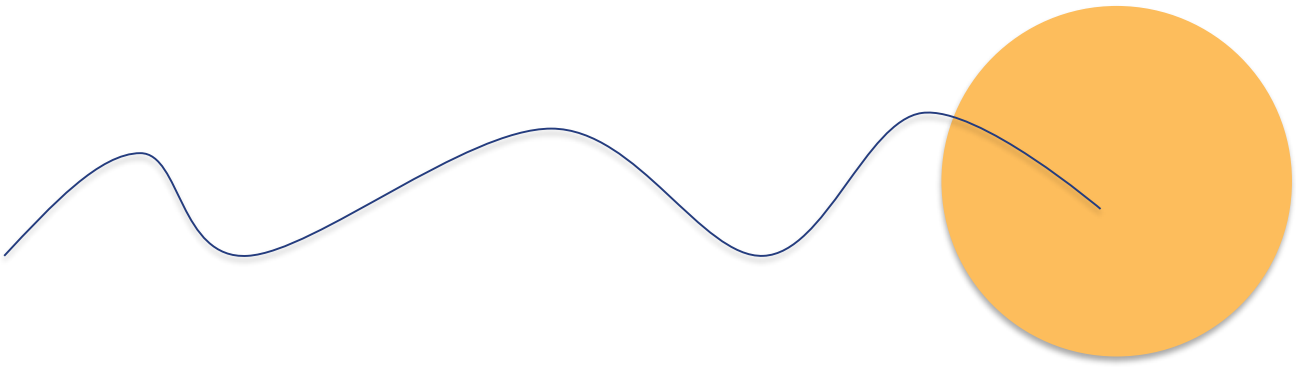
Individual Website Findings

Partidul Acțiune și Solidaritate / Party of Action and Solidarity (PAS) – unpaspentru.md

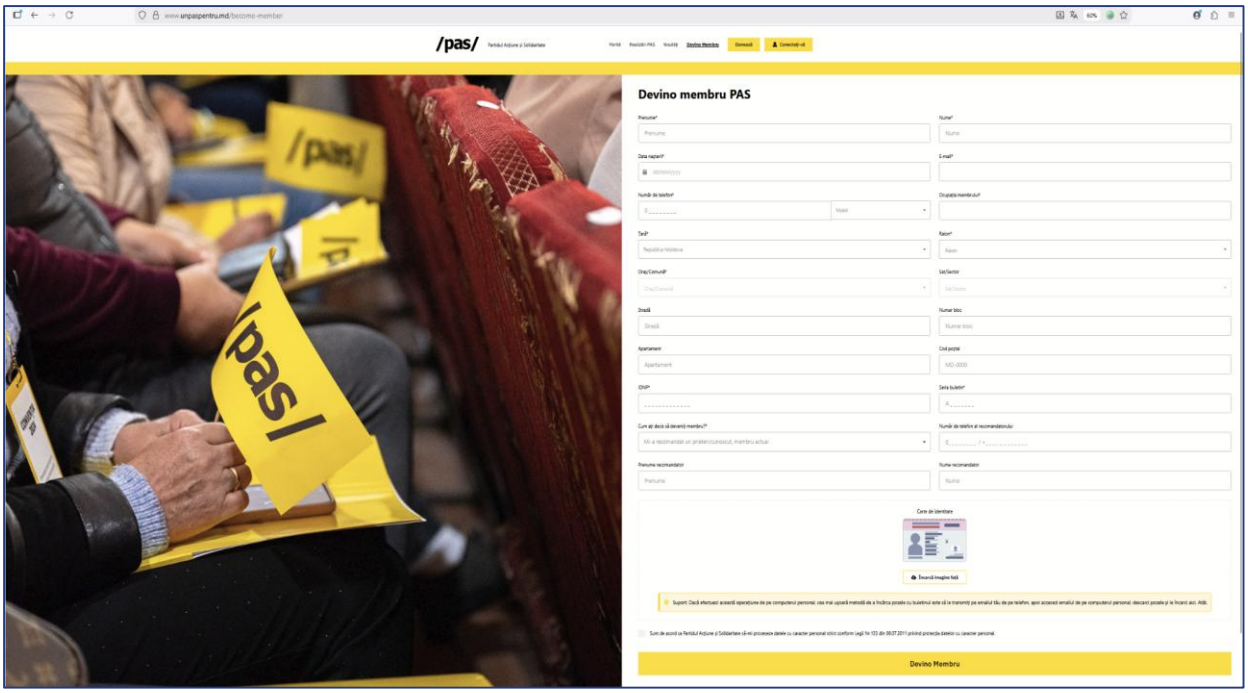
PAS operates the most functionally complex website of any parliamentary party, offering subscription to email updates, party membership applications, a donation form, a user login portal and membership fee payment functionality, and a public comment form. The site has a published Privacy Policy and Terms and Conditions. The technical analysis detected one third-party cookie belonging to a tech company Cloudflare Inc. and canvas fingerprinting – a technique designed to identify and track users even when third-party cookies are blocked. However, the website provides no cookie banner/notice for users.

Although the Privacy Policy is published and is quite comprehensive, it still fails to meet the requirements of Article 12 of Law No. 133/2011. In particular, it does not identify the data operator or authorised processors, specify data categories, purposes, legal bases, storage periods, or data subject rights, and incorrectly states that the GDPR applies directly to processing in Moldova and that Moldova is a member of the EU.

The membership application form found on the website lacks an identity verification mechanism and relies on consent as a legal basis in a context where this is legally questionable. The same deficiencies largely recur on the party's auxiliary campaign website, http://pas2025.md.

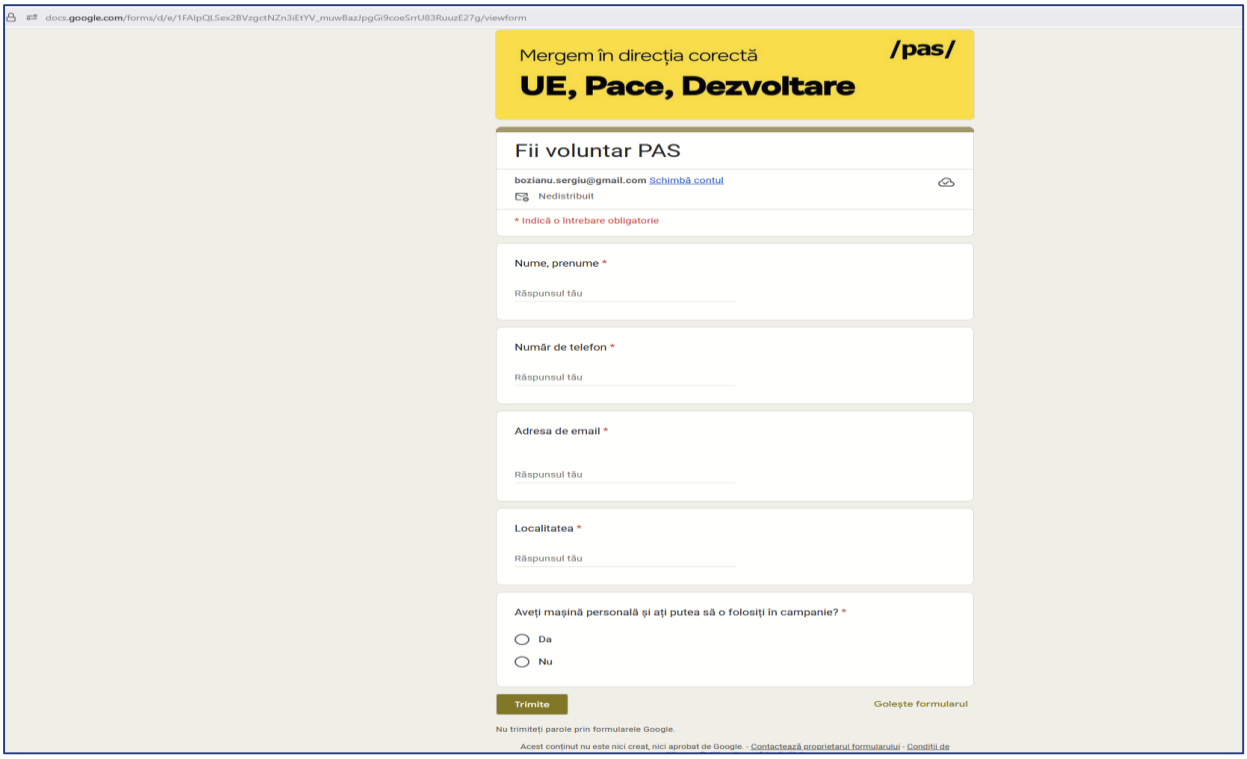


[12] The research team tested this mechanism based on its availability on the party websites, including:
https://www.unpaspentru.md/payment/donation/check-customer-data
https://pda.md/adera-la-partid/
https://partidulnostru.md/donation
https://alternativa.eu/doneaza/
https://pdcm.md/ro/donate
https://congresulcivic.md/donate/



Membership Application Form on PAS website. Screenshot as of March 6, 2026

Notably, the latter links to a Google form-based volunteer registration questionnaire, which contains no information notice on data processing and protection or asks for data subject's consent upon submission.



A Google-form-based volunteer registration questionnaire linked to on http://pas2025.md website. Screenshot as of March 6, 2026.

Partidul Socialiștilor din Republica Moldova / Party of Socialists (PSRM) – socialistii.md

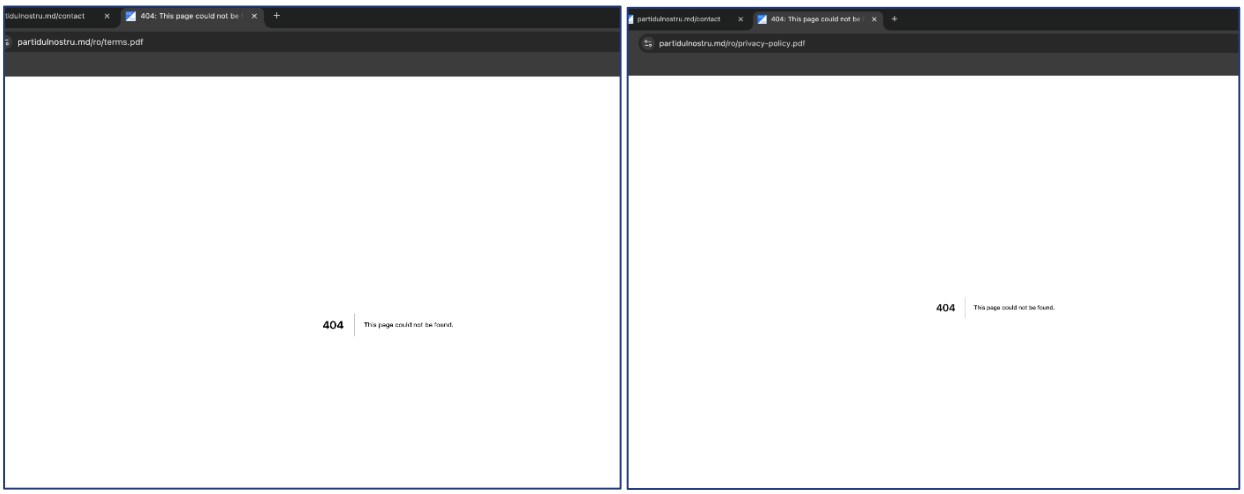
The Socialists' website is the most minimal of those analysed. Blacklight detected no third-party cookies or trackers, and the site does not appear to collect personal data through online forms (the website provides a downloadable paper membership application and contact details for regional offices). The website has no Privacy Policy of any kind, and no data processing and protection notice or a cookie banner are displayed.

According to the hosting provider company, Digital Ocean, the party's website server is located in Germany, meaning cross-border data transfers take place even in the absence of active data collection mechanisms visible to the user. The overall lack of indication that any data protection governance infrastructure is present on the PSRM's website – whether or not the party collects extensive user's personal data through it – is itself a compliance concern.

Partidul Nostru / Our Party – partidulnostru.md

Our Party's website offers a membership and staff reserve application form, a suggestion form, a feedback form, and a newsletter subscription functionality, none of which include consent mechanisms or contain an information notice on data processing and protection. Blacklight detected two advertising trackers – scripts belonging to Facebook Inc. and Alphabet Inc. – but no cookie notification is displayed on the website.

Additionally, a cross-border data transfer occurs through the use of the email address presapartidulnostru@gmail.com indicated on the website, meaning any data provided when contacting the party via a respective email address is routed through Google's servers outside Moldova. The pages displaying Privacy Policy and Terms and Conditions on the website do not load, meaning users have no accessible means of obtaining information about how their data is being processed.

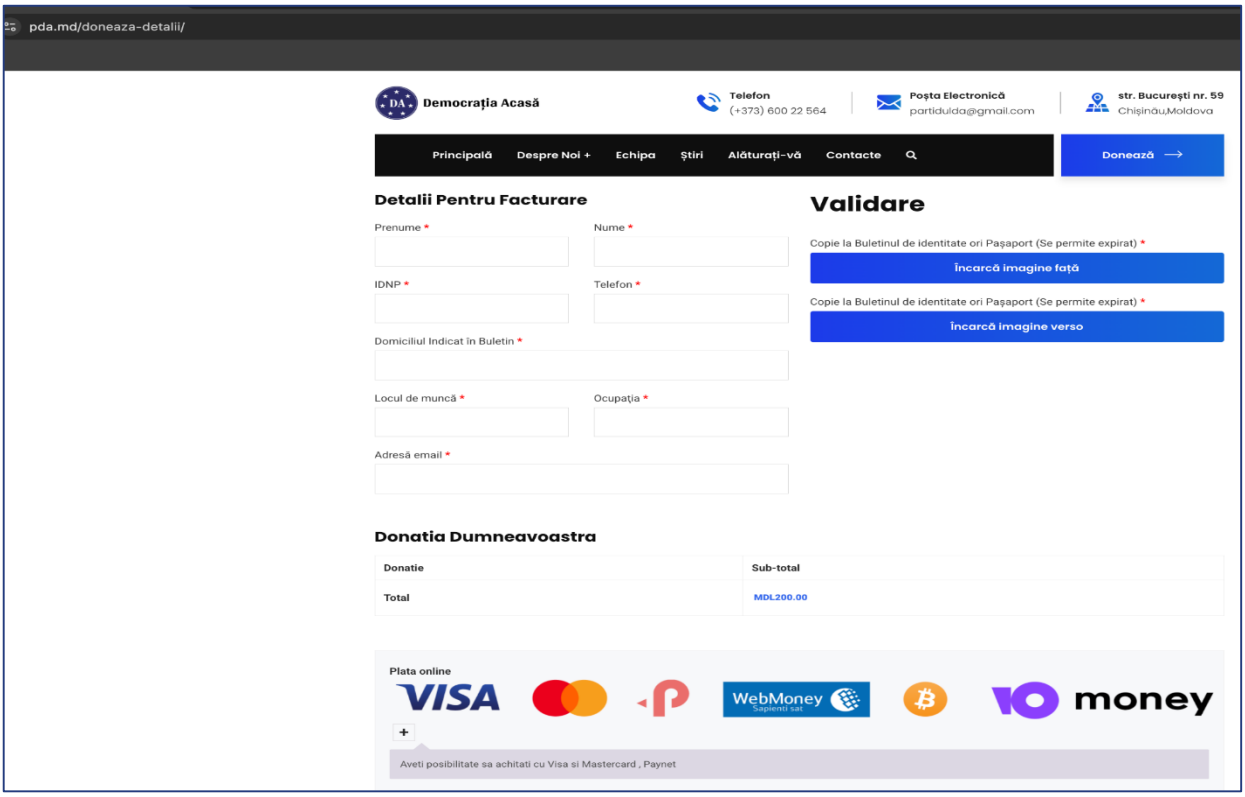


Our Party website partidulnostru.md fails to load pages displaying Privacy Policy and Terms and Conditions. Screenshots as of January 11, 2026.

Partidul Democrația Acasă / Democracy at Home Party (PDA) – pda.md

PDA's website offers a contact/feedback form, a join the party form, and donation functionality. The site carries an Alphabet Inc. advertising tracker, but no cookie notice is displayed. The party has a published Privacy Policy and Terms and Conditions; however, the Privacy Policy is assessed as formal and non-compliant, failing to specify the data operator's identity, data categories, purposes, legal bases, storage periods, or data subject rights, and containing no cookie policy. Cross-border data transfers occur through an email address partidulda@gmail.com, affecting data provided when contacting the party via a respective email address.

The donation form does not contain a mechanism for validating the IDNP and the data from the copy of the ID card, including functionality that allows collection of an erroneous copy of the identity document, and consent is wrongly invoked as the legal basis for processing donation data. The Terms and Conditions note that donation data may be shared with the CEC.

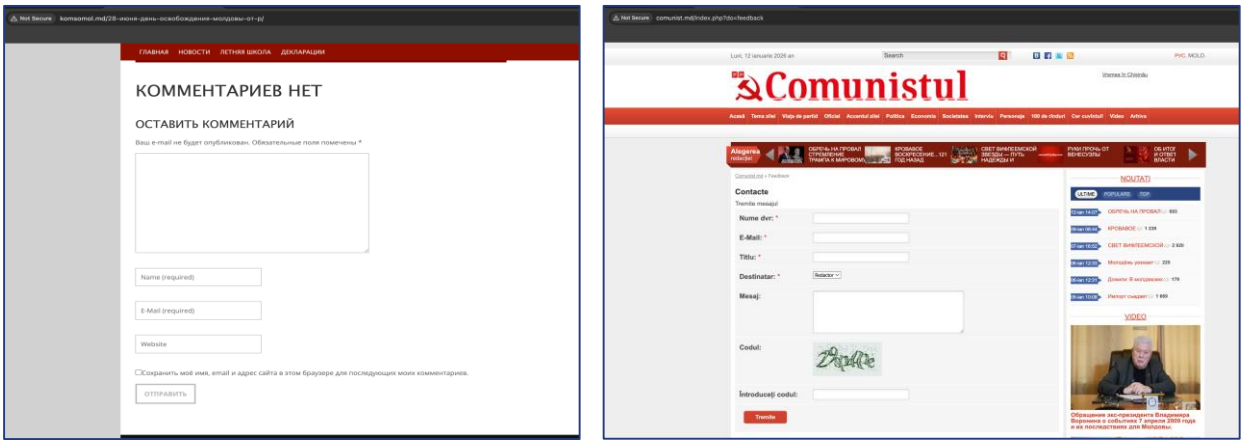


A Donation form on the PDA's website. Screenshot as of January 12, 2026

Partidul Comuniștilor din Republica Moldova / Party of Communists (PCRM) – pcrm.md

The Communists' website does not appear to collect personal data directly through forms, but embeds an Alphabet Inc. analytics script alongside four of its cookies, without displaying any cookie notification or data processing and protection notice and without offering a Privacy Policy. The site links to a youth organization website (http://komsomol.md/) and a party-affiliated newspaper (http://comunist.md/), neither of which appear to use SSL encryption; one features a commenting form that collects email addresses, and the other an editorial feedback form – both raising additional data collection security concerns outside the main party domain.

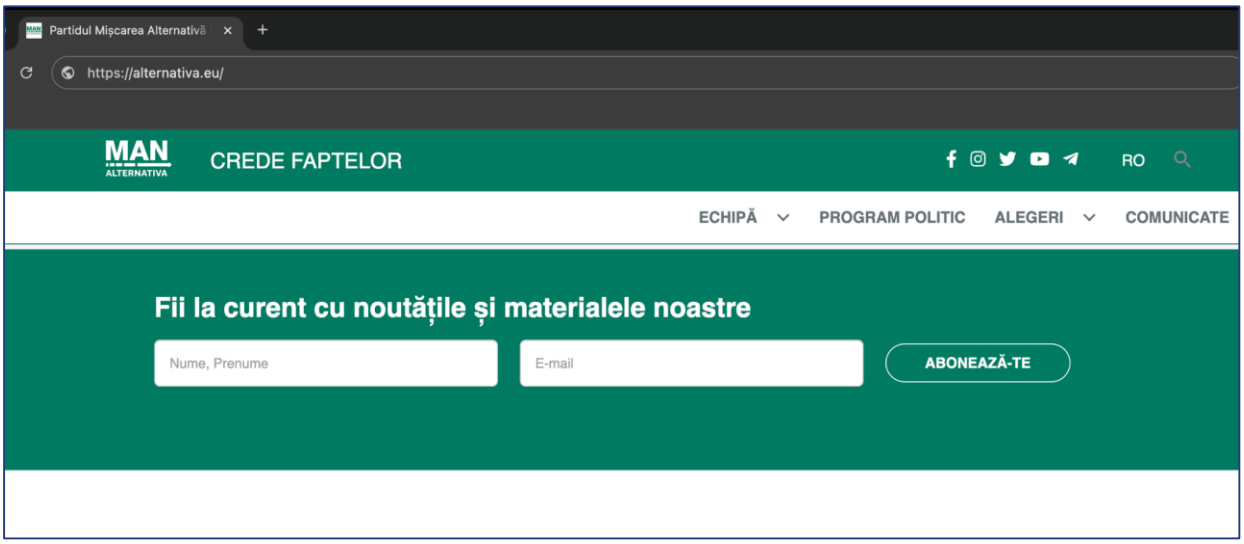
Cross-border data transfers occur through a Gmail address pressapcrm@gmail.com used for press contacts.



A commenting form on the http://komsomol.md/ website and an editorial feedback form on the http://comunist.md/ website. Screenshots as of January 12, 2026.

Partidul "Mișcarea Alternativa Națională" / National Alternative Movement Party – alternativa.eu

National Alternative Movement Party's website offers membership, volunteer registration, contact, and donation forms, with data processing and protection notices and consent windows displayed inconsistently across the three.



Newsletter subscription functionality on the National Alternative Movement Party's website https://alternativa.eu/, Screenshot as of January 14, 2026.

The Privacy Policy, dated 2022, is not prominently displayed and is not immediately identifiable as a clickable link. It is assessed as formal and non-compliant, lacking the required information on data operator identity, data categories, purposes, legal bases, storage periods, data subject rights, and cookie policy.

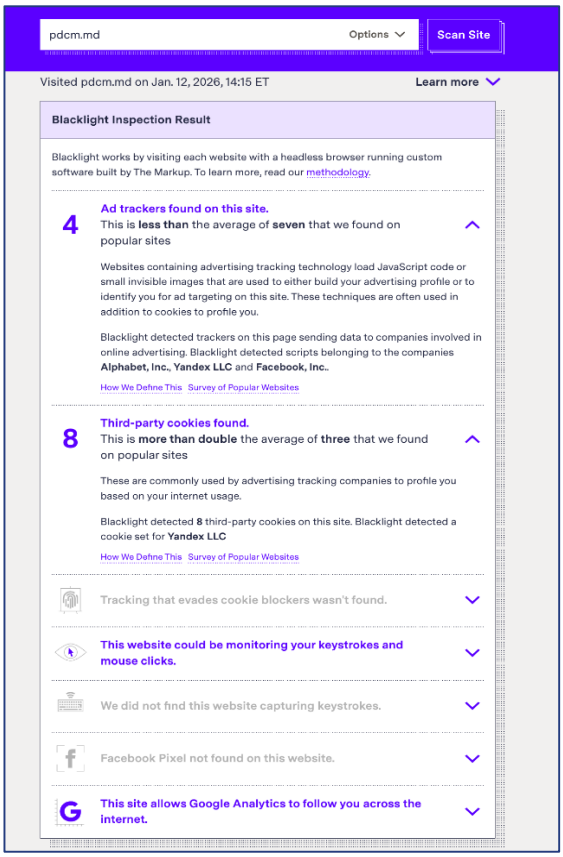
As with other parties, the donation form does not contain adequate identity verification, having been successfully completed with non-existent data and an internet image in place of a genuine ID document during testing.

Partidul Dezvoltării și Consolidării Moldovei / Party for the Development and Consolidation of Moldova (PDCM) – pdcm.md

PDCM's website presents the most significant tracking profile of any party analysed. Blacklight detected scripts belonging to Alphabet Inc., Yandex LLC, and Facebook Inc., eight third-party cookies including a Yandex cookie, and a session recorder – a tool that compiles video recordings and heat maps of user mouse movements, clicks, scrolls, and potentially network activity, including sensitive data such as passwords and payment information.

The party's donation page additionally requires users to upload a copy of their national identity card. The site has a Privacy Policy and Terms and Conditions with a consent checkbox, but the Privacy Policy seems to be identical to that of pda.md and is assessed as non-compliant in the same respects.

The site also displays two additional policy documents labelled "Privacy Policy" and "GDPR" which incorrectly apply GDPR rather than Moldovan law. Consent is erroneously invoked as the legal basis for donation processing, and donor identity is not independently verified. The use of Yandex services, including the potential session recorder, raises particular concerns given implications of the cross-border transfer to an unsafe jurisdiction and the data security risks documented in research on session recording tools.



Blacklight report of the audience analysis and tracking technology used by the PDCM on its website https://pdcm.md/. Screenshot as of January 12, 2026.

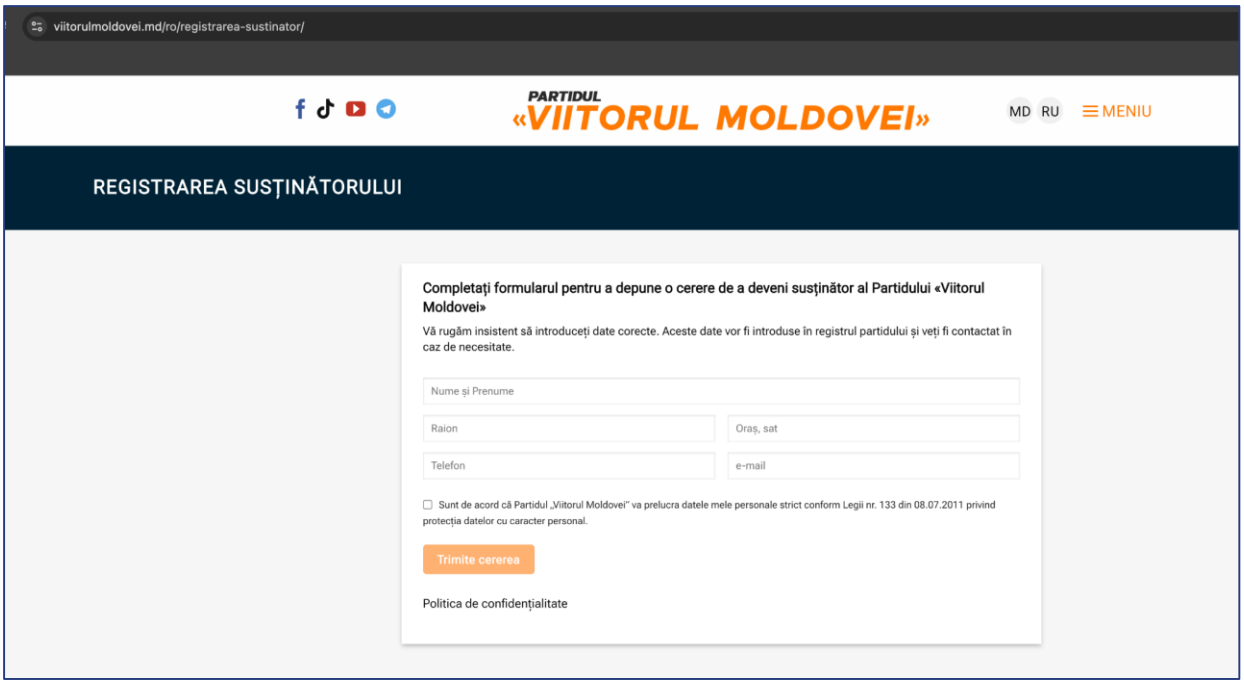
Congresul Civic / Civic Congress – congresulcivic.md

Civic Congress's website offers a join form with a consent box, a pop-up sign-up for updates, a contact form, and a donation form. The website uses an Alphabet Inc. advertising tracker. At the same time, the cookie and data processing and protection notices are absent. A reference to personal data and consent appears only in the Terms and Conditions, which a user encounters only upon initiating a donation. The donation form lacks donor identity verification mechanism. No Privacy Policy is published.

Partidul Viitorul Moldovei / Future of Moldova Party – viitorulmoldovei.md

Future of Moldova Party's website is the only one assessed as having made a genuine attempt to align its privacy documentation with Moldovan legal requirements. Each data collection form – covering membership applications, donations, public issue submissions, and questions – links to a Privacy Policy and includes a consent button and a data processing and protection notice.

However, the site nonetheless presents compliance concerns: Blacklight detected scripts from Yandex LLC and Alphabet Inc., eight third-party cookies, including a Yandex cookie, and potential keystroke and mouse-click monitoring via a Yandex script. The Privacy Policy, while more substantive than those of other parties, contains errors – most notably, it cites legitimate interest as a legal basis without adequate justification, does not address cookie configuration, and does not provide data protection officer contact details as required by Articles 25(6) and 25/1(4) of Law No. 133/2011. Like PDCM, the site's use of Yandex services raises concerns about cross-border data transfers and the adequacy of safeguards applied.



A supported registration form on the Future of Moldova party's website https://viitorulmoldovei.md/. Screenshot as of January 12, 2026

Note: During initial analysis in January 2026, the website's donation form seems to have been disabled. During a repeat analysis in February, the website did not appear to establish an SSL-encrypted connection.

2.2. Collection and Processing of Personal Voter Data: Questionnaires and Interviews

As of Feb 28, 2026, the responses to the official requests for information sent out on February 13, 2026, according to Law 148/2023 on access to information of public interest, to all nine Parliamentary parties have been provided to Promo-LEX by five parties: Partidul Acțiune și Solidaritate (PAS)/Party of Action and Solidarity, Partidul Socialiștilor din Republica Moldova (PSRM)/Party of Socialists of the Republic of Moldova, Partidul Nostru/Our Party, Partidul Dezvoltării și Consolidării Moldovei (PDCM)/Party for the Development, and Partidul Viitorul Moldovei (PVM)/Future of Moldova Party – the latter agreeing to provide the initial responses during an interview. PDCM, PSRM, Our Party, and PVM have also agreed to an interview with the research team to clarify and provide additional context to the questionnaire responses.

Based on this information, the research team has observed that while some parties openly acknowledge collecting meaningful categories of personal data – member names, IDNPs, addresses, employment data, and donor information – and describe this processing in detail – others largely disclaim personal data collection and often describe their voter outreach as purely informational (leaflets, public social media), with an exception of collecting legally mandated data, such as signatures gathered for presidential candidate nomination or member lists.

At the same time, both responses to a questionnaire and follow up interviews reveal a rather **superficial understanding of both the concept of personal data of citizens and what constitutes its processing within the framework of party activity**. For instance, in some cases, parties have demonstrated not being aware of the full extent of their existing data-based voter outreach methods – such as through digital tools. In one case, a party representative admitted not fully knowing whether the e-mail notification sign-up form on the website is currently functional or what happens with the data that is being entered through the form.

In another case, a party strongly disclaimed any personal voter data collection beyond what is strictly prescribed by law during the electoral process. However, it described a case of how local party leaders may store contact data of members or sympathisers whom they know on their personal devices (i.e., phones) and use it, for example, to invite citizens to a local party event. The respondents framed this as "personal contacts" of these individual party functionaries rather than

data held and processed by the party, since there is supposedly no centrally-operated database of such contacts. Such framing is highly problematic, as it allows the party to formally deny centralized data processing while in practice benefiting from a distributed network of contact lists used to mobilize supporters (achieving the same outcome as one would through a CRM database), without any of the accountability. From a legal point of view, the decisive question here is not *where* the data is stored or *who physically holds the device* – it is whether the data is processed in the context of, and for the purposes of, the party's political activity. Most importantly, such data almost certainly constitutes a special category of data, as a list of contacts maintained by a party branch leader and used for the purpose of inviting those people to political events is not neutral data: *it reveals, or can be used to infer, political opinions and political affiliation.*

Limited understanding (and usage) of online profiling and targeting tools: None of the parties describe using social media advertising tools, audience segmentation, or any form of digital profiling and targeting – which contrasts with practices documented in similar studies in other countries of the region. A possible explanation – as noted in one of the obtained responses – is that these activities occur through social media platforms' native tools (Meta Ads, YouTube targeting) in ways that parties do not consider "automated decision-making" within the meaning of the question. However, using public social media channels for voter outreach may still involve data processing through analytics and platform-level audience profiling even if the party does not acknowledge it as such. The same applies if parties contract social media marketing companies that purchase such services on their behalf.

Incorrectly disclaimed third-party data sharing: All respondents denied sharing voter data with third parties in ways that raise data protection concerns. However, as indicated in our analysis of political parties' websites, a variety of technological solutions that entail sharing user data with third parties (and, in some cases, across borders) are being utilized.

Largely procedural data security measures: those respondents that provided at least some details on the technical implementation of security measures, differed drastically in their description – with some describing access limitation, data accuracy controls, and updates on request, while others mentioned only "restricted access" and on-premises-only processing – a basic physical security posture.

Notably, only one party described encryption, and none mentioned pseudonymization, intrusion detection, or any other technical security measures by name – suggesting either that such measures are in place but not documented in the questionnaire or interview, or that the security posture across all surveyed parties is primarily procedural rather than technical.

Limited and formalistic compliance with data protection obligations, sometimes as a direct result of the CNPDCP audit: four out of five parties that returned the questionnaire indicated that they have an internal Data Protection Policy – with three providing a link to privacy (or confidentiality) policies on their respective websites. However, our analysis indicates that these are, in most cases, formal documents that fail to meet the minimum transparency requirements of the law (see the V. 2.1. Political Parties' Websites: What we observed for more detail). Only **one** party has provided a more comprehensive internal data protection policy for analysis within the framework of this study (developed as a result of an audit held by the CNPDCP). **Three** out of five parties that returned the questionnaire indicated that they have appointed a Data Protection Officer (but not all published their contact information online and none notified the CNPDCP). However, some of the interviews revealed a rather limited understanding of the duties of the DPO and made the assessment team question the extent to which such a designation fulfilled respective legal requirements. According to the received responses, only **two** out of five parties have conducted a Data Protection Impact Assessment: Partidul Nostru/Our Party and PSRM.

3. Central Election Commission

The request for access to information was sent to the Central Electoral Commission on 24.02.2026 and an interview with representatives of the Central Electoral Commission was also requested, which took place on 27.02.2026 and lasted for 1.5 hours. The meeting was attended by the Chair of the Central Electoral Commission – Ms. Angelica Caraman – and the person introduced as responsible for data protection, Ms. Dana Munteanu.

During the interview, the CEC leadership provided complete and equidistant information, communicating detailed answers, including specifying the challenges and problematic aspects that the CEC faces. In a follow up to the interview, Ms. Daniela Munteanu provided additional documents and information for analysis by the research team the following week.

The research team notes CEC's immediate reaction to the submitted request, as well as the participation of the CEC Chair, which demonstrates maximum openness of the CEC and their understanding of the data protection's critical importance in the electoral process.

The assessment took note of such aspects as registers and record systems held and managed by the CEC, such as: the State Register of Voters (according to Decision No. 1140/2023 for the approval of the Regulation on the State Register of Voters), the Register of Electoral Officials (according to CEC Decision No. 22/2011 on the approval of the Regulation on the Register of Electoral Officials), the register of members of political parties, reports on the financial management of political parties, auditor's reports on financial statements, reports on agreed procedures on the financial management of political parties, reports on the financing of electoral campaigns submitted by electoral competitors or referendum participants and reports on the financing of initiative groups, the register of party members, the record of observers, electoral lists, lists of candidates, initiative lists, subscription lists, information on donors and contributors, etc. Thus, there is widespread processing of the usual category and special categories of data (political views), including the processing of identifiers with a generally applicable identification function (IDNP). Moreover, in some cases, such as in the case of donors/party members and candidates, profiling (creating profiles) takes place, through which identification data (surname, first name, IDNP, home address, etc.), place of work and financial data (data on expenses and income) are collected.

Profiling also consists of processing other categories of data through Mconnect: list of payments for social benefits, social benefits of the individual, vehicle data based on the registration number, mandatory RCA insurance, data about the means of transport, state border crossings by the means of transport, bank accounts and arrears of the individual or legal entity, data about the real estate, patents of the individual, income of the individual, data about the individual, administrative offenses of the individual, state border crossings by the individual, statement from the account of the insured person, data about the legal entity.

3.1. Areas of good practice

The following areas of good practice were identified during the assessment:

The CEC has a Personal Data Protection Policy, approved several years ago. The Policy contains several rigorous requirements regarding the need to comply with data protection principles, legal bases, ensuring the rights of data subjects and includes requirements for the organizational and technical measures necessary to ensure an adequate level of protection of personal data. The policy is complemented by a detailed information notice on the processing method and the protection measures provided as well as a procedure for managing security incidents.

The CEC stated that it had designated a person responsible for data protection (DPO), in accordance with the requirements of art. 25 para. (1) of Law no. 133/2011. (See the section below for related shortcomings).

The CEC has taken measures to restrict access to the RSA: the access by authorised users of the RSA is achieved by applying strict requirements for their identification and written information on the obligation to respect confidentiality and personal data protection requirements when processing data in this register. Access rights are granted on a limited basis – each having access only to data from the constituency to which they belong. The possibility of extracting lists and personal data has

been restricted in the system, and the circle of persons who can manage the information in the RSA is as narrow as possible without the possibility of making manipulations/modifications or insertions.

All accesses made from the RSA are made through Mconnect, the accesses being displayed in the user's personal cabinet (Mcabinet and the EVO application) – confirmation of this fact is also served by those complaints and notifications that have been examined by the CEC but also by the CNPDCP. (However, the web pages managed by the CEC do not include detailed information on the way in which personal data is processed and protected by the CEC, including what the rights of data subjects are and how they can be exercised).

The CEC has modified the display of electoral lists to restrict access: approximately from 2021, the procedure for displaying electoral lists before elections has been modified. Previously, the data was displayed in electronic format for unrestricted public access to all voters with the possibility of extracting and copying these lists. Currently, this electronic format has been excluded, with each person having the opportunity to verify themselves in the RSA by entering their IDNP and the result displaying pseudonymized data (initials of the last name and first name, the last digit of the year of birth and the polling station).

The CEC has implemented depersonalization of its correspondence upon publication: published incoming and outgoing correspondence is depersonalized from personal data that are not of public interest such as: home address, signature, telephone, email, etc. The information displayed refers to the name, surname, position held by the data subject and the disposition documents issued by the CEC in relation to these needs. The analysis on a sample of 50 published documents did not establish any personal data that would have been published in violation of Law no. 133/2011.

The CEC made efforts to comply with the data retention requirements: the CEC strictly respects the deadlines provided by legislation in force, and in particular those determined by Order no. 57/2017 approved by the State Archive Service regarding the approval of indicator standard documents and their retention periods for public administration bodies, institutions, organisations and enterprises of the Republic of Moldova and the Instruction regarding the practice Indicator.

CEC-CNPDCP cooperation: the CEC had several collaborations with the CNPDCP, including notifications regarding possible cases of violations regarding the processing of personal data, in the context of keeping registers and databases.

3.2. Areas for improvement

However, during the assessment, the research team has identified the following gaps and areas requiring remedial action. Including:

Shortcomings in the Personal Data Protection Policy: CEC's current data protection policy contains references to several repealed normative acts, including some requirements that seem to be no longer relevant, especially those relating to the marking of documents, the quality of registered data controller, and issues regarding consent. It also does not contain information such as: the tasks and responsibilities of the person responsible for data protection, requirements for data protection impact assessment, requirements for subcontractors, and issues related to cross-border transfer.

No Data Protection Impact Assessment or prior CNPDCP consultation: in the case of registers and record systems, the impact assessment on personal data protection was not carried out, including at the stage of drafting and approving normative acts, in accordance with the requirements of Article 23 of Law No. 133/2011. This applies across a wide range of systems: the State Register of Voters, the Register of Electoral Officials, the register of members of political parties, financial reports, electoral lists, candidate lists, subscription lists, and information on donors and contributors, among others.

Prior consultation with the CNPDCP was also not carried out in the context of keeping registers and databases, despite several instances of collaboration having taken place.

Data Protection Officer's contact details not publicised: the contact details of the designated data protection officer have not been published on the website, at the headquarters, or at the polling stations, nor has the CNPDCP been notified, as required.

Data Protection Officer's role lacks clarification: it is necessary to clearly determine the rights, obligations and responsibilities of the data protection officer, including to exclude any possible incompatibilities in relation to the tasks of the data protection officer within the meaning of art. 25 par. (6) of Law no. 133/2011 (As a general rule, positions within the organisation with which he/she may come into conflict may include management positions (such as chief executive officer, chief operating officer, chief financial officer, chief medical officer, head of marketing, head of human resources or head of IT), but also other lower-level positions if they lead to the possibility of determining the purposes and means of processing. In addition, a conflict of interest may also arise, for example, where an external DPO is asked to represent the data subject or processor in court in cases involving data protection issues https://www.dataprotection.ro).

Website shortcomings: the web pages managed by the CEC do not include detailed information on the way in which personal data is processed and protected by the CEC, including what the rights of data subjects are and how they can be exercised.

Incidents and complaints of non-compliant processing of personal data: Several cases of notification/complaints and ex officio self-notifications by the CEC regarding the non-compliant processing of personal data were identified, with corresponding notifications being made to the General Inspectorate of Police and the CNPDCP. The cases notified to the CNPDCP were examined and resolved in a fairly extended period of time, due to the fact that the legal framework for opposition involves several activities and requirements, the processes lasting more than 6 months, and in some cases this term being even longer.

Subsequently, there were several complaints from individuals who found that the CEC accessed personal data in Mcabinet (the solution provided by the Electronic Government Agency). In practice, the access takes place in an automated manner without the involvement of the human factor – RSA consumes data on individuals from the State Population Register.

4. National Center for Personal Data Protection

The request for access to information of public interest was sent to the CNPDCP on 24.02.2026, soliciting an interview with the organization and the provision of answers to several questions related to the exercise of the CNPDCP's powers in the electoral field. The response was not provided by the CNPDCP within the legally stipulated deadline, and after several phone calls, the CNPDCP representatives agrred to an interview on 10.03.2026. The meeting was attended by two representatives of the CNPDCP: the Deputy Head of the Legal Department and the Main Controller from the same department. The interview was conducted in a hybrid format.

Incidents involving personal data processing during the electoral process

During the interview, it was established that during the last five years, the CNPDCP examined **23 cases regarding personal data processing in the electoral process**, of which: 20 cases were initiated upon the notification of the General Inspectorate of Police and two cases were initiated upon the notification of the CEC. The complaints in question claimed non-compliant processing of personal data (collection of data from unauthorized persons, collection of data for erroneous purposes, violation of the rights of the data subjects, and cross-border transfer contrary to legal requirements). Of the 23, in five cases the information was redirected to the prosecutor's office for examination according to competence.

At the same time, according to the interview, the cross-border transmission of data to the Russian Federation, carried out in violation of the requirements of Law no. 133/2011, was established **only in case of 7 persons** (the data being illegally used to open fictitious bank accounts in the Russian Federation). The practice of fictitious preliminary registration for voting in the Russian Federation was also noted and the CNPDCP submitted certain recommendations to the CEC to tighten the registration of the persons concerned. (The CNPDCP could not confirm whether the measures have been subsequently adopted by the CEC).

During the last 5 years, the CNPDCP has never applied the competence provided for by art. 6 para. (2) of Law no. 133/2011, through which it can prohibit the processing of the special category of data (political views) even when consent was granted.

The CNPDCP also reported that in recent years it has developed no instructions or guides on how to process personal data withn the framework of the electoral processes, the last instruction being approved in 2013.[13]

In the last five years, no ex officio checks exclusively at the initiative of the CNPDCP have been carried out.

The representatives of the CNPDCP also noted that in the last five years, no trainings of political parties, CEC, etc. with regard to the electoral process have been carried out, citing lack of requests. The representatives of the CNPDCP have also not participated in television, radio or mass media broadcasts to raise voters' awareness of data protection issues during elections; however, the CNPDCP issued official statements for its website and Facebook page, along with other official communication. No other special measures have been taken by the CNPDCP to ensure the compliance of data processing in the electoral sphere.

According to the CNPDCP's Activity Report for 2025, there has been an intensification of the phenomena of improper collection and use of personal data in the pre-electoral and electoral period; thus, given the multitude of situations recorded, it also issued corresponding warnings and recommendations.

Compliance of the electoral actors

Regarding the obligation to notifiy the CNPDCP on the designation of the person responsible for data protection, there have been a total of 160 notifications, of which 50 came from public authorities and 110 from the private sector. The CNPDCP has confirmed that neither political parties, nor the CEC, notified it about the designation of the person responsible for data protection (as provided for by art. 25 of Law no. 133/2011). Additionally, since 2022, no prior consultation with the CNPDCP had been requested, according to the provisions of art. 24 of Law no. 133/2011.

During the interview, the CNPDCP indicated that the current situation in the electoral field is due to the fact that political parties are not aware of the importance of data protection, and that it would be necessary to train political parties on the matter before each electoral cycle, to tighten penalties for violations, but also to improve the practice of examining violation cases in court.

Controls and supervision powers

Regarding the regulatory framework, the CNPDCP assesses that, according to Law no. 133/2011, it possesses sufficient control and supervision levers, including punitive measures. At the same time, in the previous period, there was an initiative from the CNPDCP through which certain requirements and restrictions were inserted regarding the collection of copies of identity documents by electoral actors, including measures regarding public meetings. The respective changes made to the legal framework are welcome and will bring a beneficial contribution to counteracting the phenomenon of abusive use of copies of identity documents and the administration of citizens' personal data for obscure purposes.

The CNPDCP also reported holding meetings with the CEC leadership, through which the tasks and responsibilities of these two authorities were agreed, each in its field of competence.

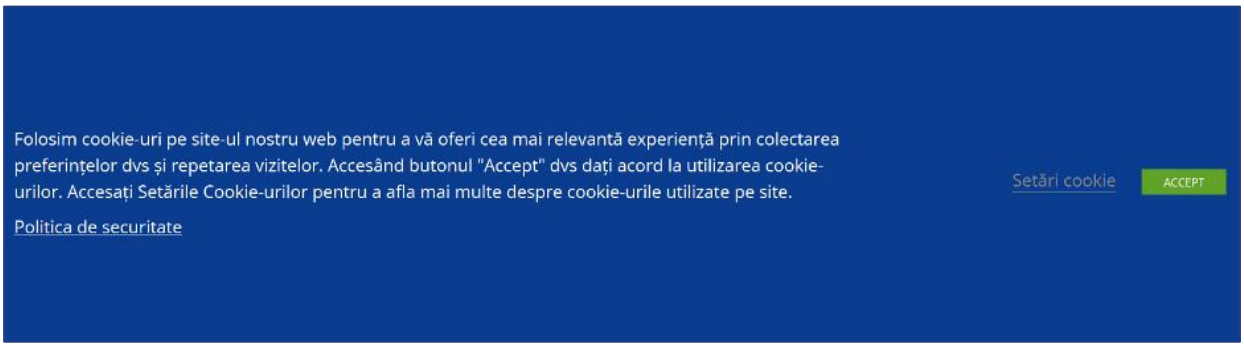
Notably, Law No. 100/2025, in force since June 2025, has introduced a new preventive enforcement tool for the CNPDCP: the power to temporarily suspend personal data processing operations where significant risks to the rights and freedoms of a large number of data subjects are identified, subject to judicial review within five days.[14]

[13] See https://datepersonale.md/wp-content/uploads/2020/01/ORDIN-nr21.pdf

[14] Data Protection and Safeguards against Voter Profiling (Articles I, VII, IX) in the OPINION ON LAW No. 100/2025 CONTAINING A SET OF LEGISLATIVE AMENDMENTS AIMING TO COMBAT ELECTORAL CORRUPTION Adopted by the Venice Commission at its 146th Plenary Session (Venice, 6-7 March 2026) https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2026)007-e

Analysis of the website

The research team has also reviewed the website **www.datepersonale.md** on March 11, 2026**.** When accessing the web page, a notification is displayed stating that the web page processes cookies. At the same time, the notification in question is positioned on 30 percent of the active screen and does not offer the possibility of closing/waiving it, the acceptance agreement being implicitly forced.



Cookie banner on the CNPDCP website www.datepersonale.md. Screenshot as of March 11, 2026

In the Security Policy section, a document is displayed, but it is not dated, which makes it impossible to determine the period in which it was approved and updated. Notably, the information displayed appears to be outdated, because this document refers to the CNPDCP's compliance with:

- Government Decision No. 1123/2010 approving the minimum security requirements for the processing of personal data – a regulatory act that was repealed at the end of 2024[15];
- Law No. 982/2000 on access to information – normative act repealed at the beginning of 2024[16];
- There are also ambiguities regarding the fact that according to the Security Policy, the CNPDCP indicates that it can process the special category of data (in our case, political preferences/political views) only based on the consent of the data subject, which can be withdrawn, thus, it is not clear whether this situation allows the CNPDCP to carry out the control of legality in the electoral field without the consent of the data subjects obtained in advance;
- It is also erroneously indicated in the Security Policy that CNPDCP would process several categories of data for registration as a personal data controller – a process that was repealed in 2022 by Law No. 175/2021.

The search engine on the website www.datepersonale.md, displayed the following results based on the keywords "electoral"; "elections"; "political parties":

- four official communiqués mentioning the participation of CNPDCP representatives in the Consultative Committee of Convention 108 in the year: 2023; 2024;
- two press releases communicating about the examination of a CEC notification (613 views) but also of a data subject regarding whom non-compliant data processing was found (190 views);
- two press releases offering the position on the statements of the Republican Party "Heart of Moldova"[17] (393 views) and the disclosure of 3,798 people[18] who are alleged to be sympathizers/activists/members of the ȘOR organization (970 views).

> **Note:** It was not possible to establish the time period of these events, because the website does not show the date of publications, which does not provide the possibility of reporting on the reference period. The same deficiencies also apply to the normative acts, recommendations, instructions and informative acts published on the website.

[15] https://www.legis.md/cautare/getResults?doc_id=145413&lang=ro#
[16] https://www.legis.md/cautare/getResults?doc_id=137924&lang=ro#
[17] See https://datepersonale.md/precizari-ale-cnpdcp-referitor-la-alegatiile-conducerii-partidului-republican-inima-moldovei-invocate-in-cadrul-briefing-ului-de-presa-din-31-martie-2025/
[18] See https://datepersonale.md/comunicat-4/

VI. Conclusions and Recommendations

1. Conclusions

The findings of this report reveal a stark and troubling disproportionality. Moldova's electoral ecosystem faces threats of documented severity – including the mass cross-border transfer of voters' personal data to the Russian Federation for the purposes of voter bribery, fictitious pre-registrations affecting tens of thousands of citizens across two consecutive electoral cycles, and the exploitation of personal data in alleged foreign influence operations. These are not theoretical risks: they are documented incidents with direct consequences for the integrity of democratic participation. Yet the actors best positioned to prevent, detect, and respond to such threats – political parties, the Central Election Commission, and the National Centre for Personal Data Protection – are, to varying degrees, struggling to meet even the foundational requirements of the current legal framework or carry out their supervisory duties.

Among parliamentary political parties, the compliance gaps identified are not merely technical. The assessment revealed that some parties demonstrate a limited grasp of what constitutes personal data and what processing operations they are already conducting – including through their own websites, digital tools, or offline practices. Four of nine parties did not respond at all to formal requests for information submitted under the law on access to public interest information. Of those that did, only two of the five respondents reported having conducted a Data Protection Impact Assessment and only one party provided a more or less comprehensive (albeit outdated) internal data protection policy for review. DPO designations, where they exist at all, appear in some cases nominal rather than substantive and no party has notified the CNPDCP of its DPO appointment.

The analysis of online data processing practices revealed that most parties published website privacy policies that are either absent, non-functional, or formal documents that fail to meet minimum legal transparency requirements. Cookie consent mechanisms are universally absent. Identity verification on donation forms is largely nonexistent. Moreover, interviews further demonstrated that party leadership is sometimes unaware of the various digital data processing mechanisms utilized by their parties, including the use of tools that entail cross-border data transfer to unsafe jurisdictions.

The CEC demonstrates greater institutional awareness, a degree of good practice, for example, in restricting access to the RSA, and a willingness to engage openly with this assessment. Nevertheless, it has not conducted a DPIA for any of the significant data processing systems it operates – including the SAISE – despite a legal obligation that has been in force since 2022. Its data protection policy references repealed legislation, the DPO's contact details have not been published, and no prior consultation with the CNPDCP has been sought.

The CNPDCP, for its part, has responded reactively rather than proactively to the documented threats. In the past five years, it has conducted no self-initiated controls in the electoral domain, issued no updated guidance for electoral actors since 2013, and provided no training to political parties or the CEC, citing lack of requests. Its own website contains cookie consent mechanisms that do not permit refusal and references regulatory acts that have since been repealed.

The periods for examining complaints – up to six months, extendable further under Law No. 195/2024 – are structurally ill-suited to the urgency of electoral violations. Thus, the CNPDCP, carrying the main role of supervision, controller, and regulator in the field of personal data protection – while mentioning in its activity reports the existence of multiple violations and complaints from the data subjects – has been practically unable to present concrete actions undertaken in the last five years that could make a significant contribution to combating the phenomenon of personal data misuse in the electioral context. This indicates that the strategy adopted for managing these incidents is inefficient and lacks impact, especially since, predominantly, the actors involved in the electoral field have reported little to no interaction with the CNPDCP (controls, training, methodological guides).

Observed mitigation measures, such as publishing on the website brief information of a general nature and initiating controls in relation to political parties predominantly upon notifications from

the Police Inspectorates and the CEC, call for a review of the CNPDCP's priorities in its role of a control and supervision entity vested with coercive force.

These findings collectively point to a systemic gap between the scale of the threat and the state of institutional readiness. The transition deadline of 23 August 2026, when Law No. 195/2024 enters into full force, represents both a binding obligation and a narrowing window for reform. Without concerted, coordinated, and proactive action across all three institutional actors assessed in this report, the risks to Moldovan voters' personal data – and to the integrity of the electoral process – are likely to persist and, absent corrective measures, potentially intensify in future electoral cycles.

It is acknowledged that the Republic of Moldova has taken some legislative steps to address electoral data misuse since the incidents documented in this report. The new Law No. 195/2024 has aligned the overall data protection framework closer to the GDPR standards, while the Law No. 100/2025, in force since June 2025, introduced restrictions on the mass collection of identity document copies, data minimisation requirements for signature-gathering activities, and a new preventive suspension power for the CNPDCP[19]. These are meaningful additions to the legal framework. More fundamentally, the findings of this report demonstrate that legislative reform is insufficient on its own: the tools introduced by Law No. 100/2025 remain untested in practice, and their effectiveness depends entirely on the institutional capacity of electoral actors and proactive enforcement posture of the CNPDCP and other relevant authorities.

In conclusion, we note that although approximately five months remain until the entry into full force of Law No. 195/2024, at the moment there is no clear intention of the authorities concerned: the CEC and CNPDCP to conduct a cross-sectional analysis of the entire legal framework affecting the electoral field, in order to introduce amendments and bring the regulation into line with the new requirements in the field of personal data protection.

We also note deficiencies in ensuring the principle of transparency and access to information of public interest on the part of some political parties and the CNPDCP, which did not demonstrate a proactive attitude in responding to these requests, even though several follow up contacts took place. (The absence of their reaction being justified by the lack of necessary personnel, engagement in some more important processes, or insufficient financial resources – but also, in some cases, the information providers were surprised that they would be obliged to respond to such requests in the first place). Thus, this demonstrates insufficient understanding and fulfillment of the legislation on access to information and transparency in the decision-making process.

2. Recommendations for political parties

1) **Adopt internal data protection policies that reflect actual practices:** Where parties have adopted internal data protection policies, these should be substantive documents that accurately describe existing processing operations, establish documented procedures for responding to data subject rights requests, set out data retention schedules and deletion procedures, define training requirements for staff handling personal data, and address incident response including breach notification to the CNPDCP within the 72-hour window required under the prospective Law No. 195/2024.

   Parties should review their *actual personal data processing practices* and explicitly recognize those in place as such – be it the usage of e-mail marketing or audience analysis tools on their websites or maintenance of member or supporter records on party officials' personal devices – and adopt clear internal policies that address such practices, ensruing that members handling such data understand their obligations. Where various informal arrangements are in place, parties should consider whether centralised governance of data (i.e., a centralized supporter or donor database) – with appropriate accountability structures – would better serve both compliance and voter rights than the current practices.

[19] However, as the Venice Commission has noted, key definitional gaps in the law – including the undefined scope of "frequent" and "mass" collection – create legal uncertainty that requires clarification https://www.venice.coe.int/webforms/document

2) **Appoint a substantively qualified Data Protection Officer, publish their contact details, and notify the CNPDCP:** Parties are required by Law No. 133/2011 to designate a DPO – which includes those processing political opinion data at any meaningful scale, including through membership registers – must ensure that any appointed DPO has the legal and technical knowledge required by Article 25(4) of the Law, understands their duties, and is genuinely involved in compliance oversight. Formal designation without substantive engagement does not satisfy the legal requirement. Contact details for the DPO must be published on party websites and provided to the CNPDCP, and the DPO must be given the organisational access and support necessary to perform their role.

3) **Conduct Data Protection Impact Assessments for high-risk processing operations:** Under both Law No. 133/2011 and (from 23 August 2026) Law No. 195/2024, DPIAs are required for processing operations that carry high risk to data subjects' rights – including, specifically, maintenance of member registers, website functionalities involving cookies and donation processing, and any interaction with supporters that may reveal or allow inference of political opinions. Parties that have not conducted DPIAs for these operations should do so before the transition deadline, with DPO involvement as required by law, and should document and act on the results.

4) **Establish and publish substantive, legally compliant privacy policies on their websites**: All parties that currently lack publicly accessible privacy policies – or whose published policy does not meet the minimum transparency requirements of Law No. 133/2011 – should, as a priority, adopt and prominently display a substantive privacy notice on their websites. That notice must, at minimum, identify the party as data controller, name any authorised processors, specify the categories of personal data collected, the purposes and legal bases for each processing operation, data retention periods, data subject rights and how to exercise them, and the contact details of the data protection officer. A layered approach – a concise first layer with a link to the full policy – is advisable given the volume of information required. Maintaining a policy that is a copy of another party's document does not reflect all data processing that takes place via the website, or one that applies the wrong legal framework, does not satisfy this obligation.

5) **Implement compliant cookie notices and consent mechanisms:** The near-universal absence of cookie banners and consent mechanisms across party websites is a direct violation of Law No. 284/2004 on information society services. All parties deploying third-party tracking scripts – including analytics tools and advertising trackers from Google/Alphabet, Facebook/Meta, and Yandex – must implement compliant cookie notices that clearly inform users which cookies are in use, their purposes, and who operates them, and that give users a genuine choice to accept or refuse non-essential cookies before those cookies are activated. This is not a technical formality: it is a prerequisite for the lawful processing of website visitors' data.

6) **Audit and govern third-party data sharing arrangements:** All parties that use third-party digital services – including cloud-based forms, email platforms, analytics providers, and social media tools – should conduct a structured audit of what data flows to those third parties, on what legal basis, under what contractual terms, and to what jurisdictions. The use of Gmail addresses as official party contacts, for example, constitutes a cross-border data transfer that must be disclosed and justified. Where parties engage data processors, written data processing agreements meeting the requirements of the applicable law are mandatory.

   a. **Urgently address the use of Yandex or other third-party services that involve data transfers to jurisdictions without an adequate data protection framework:** Parties using Yandex analytics, advertising trackers, or session recording tools – particularly where this includes potential keystroke and mouse-click monitoring – face compounded risks: cross-border data transfers to servers in a jurisdiction without an adequate data protection framework, data security risks documented in research on session recording tools, and, given the geopolitical context relevant to Moldova, heightened risks of exploitation. These services should be reviewed immediately with a view to discontinuation or replacement, and any cross-border transfers currently occurring must, in the interim, be disclosed to users and backed by appropriate safeguards.

b. **Remove or properly safeguard session recording tools:** The use of session recording technology – which can capture user keystrokes, mouse movements, and potentially sensitive form entries including passwords and payment information – carries particular risks when deployed without user knowledge or consent. Where any such tool is identified during a website audit, it should either be removed or, at a minimum, fully disclosed in the privacy and cookie notice, with meaningful consent obtained before activation. A Data Protection Impact Assessment is required before any such tool is re-deployed.

7) **Correct the misuse of consent as a legal basis:** Several parties invoke consent as the legal basis for processing in contexts where it is either inapplicable or improperly obtained – most notably in relation to donation data and membership records. Parties should carry out a careful review of each processing operation and identify the correct legal basis under Law No. 133/2011 (and, prospectively, Law No. 195/2024). Where consent is in fact the appropriate basis – for example, for newsletter subscriptions or certain campaign communications – it must be freely given, specific, informed, and unambiguous, and parties must maintain records of it and provide a mechanism for its withdrawal. Where a different basis applies (such as legal obligation or legitimate interest), it must be accurately identified and stated in the privacy notice, with legitimate interest claims supported by a documented balancing test.

8) **Adopt robust identity verification on donation forms:** Multiple donation forms were found to lack meaningful identity verification mechanisms – in at least one instance, the form was successfully completed with fabricated data and a random image. Given that donation data is subject to both data protection obligations and electoral finance transparency requirements, and that the Electoral Code requires reporting of donor identity details to the CEC, parties must implement verification mechanisms that are adequate for the legal purposes the data serves (with the guidance and support from the CEC and CNPDCP). Collecting identity document copies without verification is not a substitute for verification, and may itself represent disproportionate data collection where simpler alternatives exist.

9) **Raise party officials' awareness about data protection and prepare proactively for Law No. 195/2024:** The transition deadline of 23 August 2026 is approaching within a single electoral cycle. Parties should treat the period between now and that deadline as a structured compliance window rather than a grace period. In practical terms, this means: reviewing existing processing operations against the GDPR-aligned requirements of Law No. 195/2024; updating privacy notices, consent mechanisms, and DPO arrangements accordingly; carrying out or completing DPIAs for high-risk operations; and establishing or strengthening the internal governance capacity – trained staff, documented procedures, audit records – that the new law will require from all data controllers.

10) **Respect the legal framework for access to information:** Political parties must establish internal procedures to ensure that the legal framework for access to information is respected, that the conditions for reviewing data access requests are met, that contact information on the website is updated, and that such requests are given priority consideration as being in the public interest.

3. Recommendations for the CEC

1) **Designate a person responsible for data protection (DPO) fully in accordance with the requirements of art. 25 and 25/1 of Law no. 133/2011**, with established job description requirements, effective involvement in the decision-making process, reporting to the highest level of management; display DPO's contact details on the website, at the headquarters, and in the polling stations.
2) **Conduct data protection impact assessments** in the case of issuing administrative acts of a normative nature that involve the processing of personal data, including within managed record systems and data flows such as: RSA, Correspondence Management, video surveillance, records of financial reports, electoral lists, subscription lists, records of observers, electoral employees, party members, etc.
3) Following the data protection impact assessment, in cases of identification of high risks, **conduct a prior consultation with the CNPDCP**.
4) **Adjust existing Personal Data Protection Policy to the current legal framework**: Law no. 133/2011 on the protection of personal data, Law no. 148/2023 on access to information of public interest, Law no. 108/2025 on open data and the reuse of public sector information, but also the connection to the new legal framework – Law no. 195/2024 on the protection of personal data (among the most important: data protection principles, legal grounds, appropriate organizational and technical measures, implementation of the privacy by design and privacy by default principles, holding data processing activities). An additional remedy would be certification to ISO 27001 and 27701 standards.
5) **Develop and implement an annual training plan for employees** in the field of personal data protection, as well as for electoral staff and political parties.
6) **Harmonize the secondary regulatory framework in conjunction with the new legal framework** – Law No. 195/2024 on the protection of personal data.
7) **Consider implementing additional organizational and technical measures** for tightening access and security of the RSA.
    a) 'Verify yourself' function in the RSA https://verifica.cec.md/ – by including identification and access limitation measures, for example by confirming the OTP code; implementing trusted solutions within the meaning of Law No. 124/2022 on trusted services and electronic identification, including remote identity identification solutions (EKYC) – enforceable remedies also in the case of prior registration to exclude the malign phenomenon of fictitious voter registrations and the misuse of personal data;
    b) Tightening measures for the use of RSA (mandatory annual training, conducting security and compliance audits to verify how registrars use electronic signatures and this State Register, with random checks to determine the purpose and legal basis);
    c) Completing the issued normative acts with organizational and technical measures, in the case of keeping the RSA, the Register of Party Members, and records regarding financial reporting, subscription lists, electoral lists, etc.
8) **Update the CEC website to include:** cookie banner, the information notice on the data processing and protection, Terms and Conditions of use of the website in accordance with the provisions of art. 10 of Law no. 284/2004 and art. 12 of Law no. 133/2011.
9) **Strengthen collaboration with the CNPDCP**, in order to develop guides, instructions and informative and methodological materials regarding raising awareness of the field of personal data protection among voters, political parties, and electoral staff.
10) **Determine mandatory processes to verify the identity** of electoral staff and election observers, in order to avoid or exclude the fraudulent use of false identities.

4. Recommendations for the CNPDCP

1) **Initiate the process of amending the regulatory framework affecting the electoral sector** to comply with Law No. 195/2024 on the protection of personal data applicable from 23.08.2026;
2) **Further strengthen the collaboration with the CEC**, particularly, on the following topics: approving normative acts by the CEC, recommending certain organizational and technical measures regarding the electoral process, which would target prior voter registration, publication of electoral lists, management of financial reports, subscription lists, party members, effective beneficiaries, training of CEC members and electoral staff;
3) **Instruct political parties and summon them regarding key obligations**: the designation of the person responsible for data protection, conducting the data protection impact assessment, holding prior consultation with the CNPDCP;
4) **Develop methodological guides on how to implement the requirements of Law No. 195/2024**;
5) **Implement website updates** regarding:
    a. Updating the cookie notification, providing a cookie rejection button;
    b. Updating the Security Policy displayed on the web page and excluding outdated sending rules;
    c. Providing the web page with additional functionalities that could determine the date and time of displaying press releases, documents, recommendations, etc.;
6) **Carry out planned checks/investigations in the context of data processing in the electoral sector**;
7) **Develop CNPDCP guidelines on how to exercise the powers provided for by Law No. 100/2025**;
8) **Initiate specific steps towards all actors involved in the electoral field** regarding the need to develop personal data protection policies and the necessary organizational and technical measures according to the new legal framework on data protection; **establish the action and reporting calendar for the targeted actors**;
9) **Carry out practical "From theory to practice" trainings with responsible persons from political parties and the CEC**, presenting the necessary solutions to bring data processing operations into line with the requirements of the legal framework;
10) **Approve and post on the website the training plan** required for prevention in priority areas;
11) **Adopt necessary procedures to prioritize the examination of requests for access to information of public interest**, respect the examination deadlines, and designate the person responsible for managing requests for access to information.

5. Recommendations for the Parliament of the Republic of Moldova

1) **Reduce the period for carrying out checks** provided for in Law No. 195/2024 from 12 months to 45 days for cases notified within electoral processes or involving the systematic and large-scale processing of personal data;
2) **Amend Law no. 100/2017 on normative acts**, by introducing a new chapter in which requirements are expressly stipulated for all types of normative acts that establish, modify or regulate registers, databases, record systems or other types and structured series of personal data, to incude:[20]

[20] in accordance with art. 9 of Convention no. 108/1985 for the protection of individuals with regard to the processing of personal data, the provisions and/or art. 11 of the modernized Convention that was signed on 09.02.2023, as well as art. 23 of Law no. 195/2024 on the protection of personal data.

"Ensuring the right to privacy in relation to the processing of personal data"

(1) The regulatory acts involving the processing of personal data in registers, information systems, databases, record systems or other types of structured series, both on paper or in electronic format, will contain:

a) The purposes for which the data may be processed;
b) The data categories or types of categories considered;
c) The grounds on which personal data may be processed;
d) Data storage period;
e) Recipients or categories of recipients of the data;
f) Applicability of data subjects' rights;
g) Other important aspects in accordance with Law No. 195/2024 on the protection of personal data.

(2) The rights and obligations provided for by Law No. 195/2024 on the protection of personal data may be restricted only for the purposes provided for in Article 23 paragraph (1) of Law No. 195/2024 on the protection of personal data, such as: national security; defense; public security; prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including protection against and prevention of threats to public security; other important objectives of general public interest of the Republic of Moldova, in particular an important economic or financial interest of the Republic of Moldova, including in the monetary, budgetary and fiscal areas and in the field of public health and social security; protection of judicial independence and judicial proceedings; prevention, investigation, detection and prosecution of ethical violations in the case of regulated professions; monitoring, inspection or regulatory function related, even occasionally, to the exercise of official authority in the cases mentioned earlier; protection of the data subject or of the rights and freedoms of others; enforcement of civil law claims.

(3) In the situations provided for in paragraph (2), the regulatory act establishing these restrictions shall mandatorily contain: the purpose of the processing or the categories of processing, the categories of personal data, the scope of the restrictions introduced, the guarantees to prevent abuse or unlawful access or transfer, the indication of the operators or types of operators, the storage period and the applicable guarantees taking into account the nature, scope and purposes of the processing or the categories of processing, the risks to the rights and freedoms of the data subjects, the right of the data subject to be informed of the restriction, unless this may prejudice the purpose of the restriction.

(4) The normative acts will be subject to approval by the National Center for Personal Data Protection, Associations specialized in the defense of the right to privacy, civil society, and the business sector.

Additionally, we note that in accordance with art. 23 of Law no. 133/2011 on the protection of personal data, in the process of approving and adopting laws, an impact assessment on data protection should be carried out. (Which is an obligation that falls to subjects with the right of legislative initiative that promote draft laws with the insertion of the corresponding amendments to Law no. 797/1996 for the adoption of the Rules of Procedure of Parliament). We further note that the Parliament must designate the person(s) responsible for data protection (DPO) to carry out the tasks provided for in art. 25/3 of Law no. 195/2024, to ensure the activities of the Secretariat of the Parliament and of the Parliament of the Republic of Moldova comply with the requirements in the field of personal data protection. The contact details of the DPO must also be published.

Finally, we recommend to consider changing the parliamentary committee responsible for reporting on the activity of the CNPDCP from the Committee on National Security, Defense and Public Order to the Committee on Human Rights and Interethnic Relations, given that the CNPDCP is not a police body or one in the field of national defense and security, but is an institution for the defense of human rights.

VII. Annexes

Annex 1: Regulatory and Legal Framework

1. Applicable laws and regulations (unofficial translation)

Currently, the processing of personal data in the electoral sector is regulated by a set of normative acts specified below, which determine the conduct of political parties but also of the control and supervision bodies the CEC and the CNPDCP.

National Legislation

Law No. 133/2011 – Law No. 133/2011 on the protection of personal data (in force until 23 August 2026).
Law No. 195/2024 – Law No. 195/2024 on the protection of personal data (in force from 23 August 2026, replacing Law No. 133/2011).
Electoral Code – Electoral Code, approved by Law No. 325/2022.
Law No. 148/2023 – Law No. 148/2023 on access to information of public interest.
Law No. 294/2007 – Law No. 294/2007 on political parties.
Law No. 71/2007 – Law No. 71/2007 on registers.
Law No. 142/2018 – Law No. 142/2018 on data exchange and interoperability.
Law No. 467/2003 – Law No. 467/2003 on informatization and state information resources.
Law No. 100/2025 – Law No. 100/2025 for the amendment of certain normative acts (efficient combatting of the phenomenon of electoral corruption and related aspects).
Law No. 109/2024 - Law No. 109/2024 the partial implementation of voting by correspondence.

CEC Decisions and Regulations

Decision No. 1102/2023 – Decision No. 1102/2023 for the approval of the Regulation on financing the activity of political parties.
Decision No. 1153/2023 – Decision No. 1153/2023 for the approval of the Regulation on the preparation, administration, dissemination and updating of electoral lists.
Decision No. 1140/2023 – Decision No. 1140/2023 for the approval of the Regulation on the State Register of Voters.

International Instruments

GDPR – Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
Recommendation Rec(2003)4 – Recommendation Rec(2003)4 of the Committee of Ministers to member states on general rules against corruption in the financing of political parties and electoral campaigns.

International Guidance Documents

Opinion 05/2014 – Article 29 Data Protection Working Party – Opinion 05/2014 on anonymization techniques.
Opinion 4/2007 – Article 29 Data Protection Working Party – Opinion 4/2007 on the concept of personal data.
Opinion 1/2010 – Article 29 Data Protection Working Party – Opinion 1/2010 on the concepts of "controller" and "person empowered by the controller".

Opinion 06/2014 – Article 29 Data Protection Working Party – Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC.
Guidelines on the Protection of Individuals with regard to the Processing of Personal Data by and for Political Campaigns adopted by the Committee of the Convention for the protection of individuals with regard to the automatic processing of personal data (Convention 108), on 19 November 2021.
Handbook – Handbook of the European Data Protection Legislation.

2. Data collection and record-keeping requirements for political parties (unofficial translation)

Political parties process personal data relating to party members, party supporters, donors, and contribution payers. The following legal requirements apply to political parties as personal data controllers under the applicable laws and regulations listed above.

Law no. 294/2007 sets forth the manner of establishment, organization, management and control, rights and obligations of political parties. Thus, political parties are established as voluntary associations that are obliged to hold:

1) **The list of party members** (for registration purposes) drawn up based on applications for party membership: surname, first name, gender, date of birth, domicile, series and number of the identity document and the member's signature and the declaration of the person who drew up the respective list and who attests to the veracity of the information and signatures.
2) **Register of Party Members** (for ongoing record keeping)**,** which includes the following categories of personal data: name, surname, date of birth, state identification number, declared home address, date of registration in the register, date of suspension or termination of membership of the political party, it being expressly mentioned that the executive body of the party is responsible for the correctness of the data and information entered as well as their presentation to the CEC.
3) **Records of contributions** and the people who made the contribution, where the person's identification data and bank details are processed.
4) **Records of donations** and the people who made the donation made by bank transfer or, in the absence of a bank account, by depositing it at the party headquarters, where the donor's identification and bank details are processed, as well as holding the citizenship of the Republic of Moldova, reaching the age of 18, including data on prohibitions: people who have not reached the age of 18, foreign citizens, stateless persons, anonymous persons and people who donate on behalf of third parties, as well as the amount of donations and the established limit criteria (data on income).
5) **The financial management report**, which includes: the amount, the name and surname of the donor/contributor, the state identification number (IDNP), the domicile, the day, month and year of birth, the place of work, the position held (occupation/type of activity), as the case may be, the party membership, the sources of income or financing of the donor.

The Law No. 249/2007 does not determine specific requirements that need to be ensured in terms of the protection of personal data and the protection of other information with limited accessibility, being limited to providing that political parties must comply with the legislation of the Republic of Moldova and statutory provisions and are responsible for the correctness and veracity of the data. In turn, the Electoral Code determines and completes the method of processing personal data in the electoral field, including following obligations for the political parties:

6) **Support List of Candidates** – Political parties that submit support lists of candidates for the position of President of the Republic of Moldova and of the independent candidate for the position of deputy of the Parliament of the Republic of Moldova must include: the elective position for which signatures are collected, supporter data, the candidates' last and first names, year of birth, profession, position, place of work and the subject that designated it, as well as the collector's last and first names.

7) **Candidate Registration Data** – The information that needs to be submitted to the CEC for registration by electoral contestants includes: biographical data of the candidate, declaration of assets and personal interests, health certificate of the candidate for the position of President of the Republic of Moldova, copy of the diploma, copy of the identity document, other information regarding any restrictions.

8) **List of Initiative Groups** – The content of the lists of initiative groups for supporting the independent candidate for the position of deputy, the initiative groups for initiating the republican/local referendum, include: surname, first name, year of birth, domicile and signature of the participants.

9) **List of supporters (sympathizers) of political parties -** In this context, data such as: name, surname, data from identity documents and contact details are processed.

3. Data collection and register management requirements for the CEC (unofficial translation)

The Central Electoral Commission (CEC) acts as a personal data controller in the electoral sector, in particular:

1) **State Register of Voters** (RSA) is established and administered by the CEC according to the Electoral Code; CEC Decision No. 1140/2023 and includes the following data sourced from the State Register of Population via Mconnect: surname, first name, date, month and year of birth, IDNP, gender, home address, residence address, series and number of the identity document, number of the polling station where the voter is assigned according to their home address or where they expressed their will to vote, date of the last modification of personal data, mentions regarding persons who have lost their voting rights, other mentions.

The data from the RSA is intended exclusively for electoral processes. Each voter may access only their own personal data through the CEC website.

2) **Basis Electoral Lists** are maintained and administered by the CEC in accordance with the Electoral Code; CEC Decision No. 1153/2023 and include the following information: name, surname, locality and number of the polling station, surname, surname, year of birth of the voter, domicile/residence, IDNP and series and number of the identity document, signatures of the members of the electoral bureau and voters. In addition, information is held on persons performing military service, who are in sanatoriums, rest homes, hospitals and other stationary institutions.

The CEC must make electoral lists available to voters in polling stations no later than 20 days before election day. These lists contain: Name and surname, year of birth, domicile/temporary residence.

Access to these lists is also provided to representatives of electoral contestants, referendum participants and observers for the purpose of verifying the correctness of the data.

3) **Financial reporting data** – Based on Law No. 294/2007; CEC Decision No. 1102/2023, the CEC must process and publish data from the financial management reports of political parties on its official website. Within 48 hours of receiving the reports, all information contained in the reports of political parties regarding accumulated income and incurred expenses is published on the website of the Central Electoral Commission, except for the personal identification number (IDNP) of individuals, as well as their date and month of birth, domicile, or temporary residence.

The IDNP is not published on the CEC website.

4) **Data for the registration of electoral contestants** – The CEC must collect and process the following information submitted for the registration of candidates:

- **Support List of Candidates**: the elective position for which signatures are collected, the candidates' last and first names, year of birth, profession, position, place of work and the subject that designated it, as well as the collector's last and first names.
- **Candidate Registration Data**: biographical data of the candidate, declaration of assets and personal interests, health certificate of the candidate for the position of President of the

Republic of Moldova, copy of the diploma, copy of the identity document, other information regarding any restrictions.

- **List of Initiative Groups**: surname, first name, year of birth, domicile and signature of the participants in the assembly.

4. Data protection obligations

It must be noted that the Electoral Code and CEC Decisions No. 1153/2023 and No. 1140/2023, as well as other normative acts issued by the CEC, generally determine the need to comply with the requirements in the field of personal data protection, but without clarifying the purposes for which data may be processed, the term of storage of personal data and the process of deleting/destruction of personal data upon achieving the purposes of processing, requirements regarding the need for periodic training in the field of personal data protection, the need to carry out an impact assessment on protection, depersonalization and/or pseudonymization of data, designation of the person responsible for data protection, keeping records of audit records, the manner in which the rights of data subjects must be achieved, requirements regarding cross-border data transfer.

The Law No. 71/2007, Law No. 467/2003, and Law No. 142/2018, in the case of keeping state registers and managing data flows, determine the obligation to specifically regulate the rights and responsibilities of holders, possessors and registrars of state registers, but also in particular the measures for the protection of personal data and requirements for data confidentiality and security, including measures against destruction, modification, blocking, copying, dissemination, as well as against other unlawful actions, measures intended to ensure an adequate level of security with regard to the risks presented by the processing and the nature of the data processed.

In addition to the reference provisions, the processing of personal data is regulated by Law No. 133/2011 on the protection of personal data – a regulatory act that will be in effect until 23.08.2026, and starting from this date, the aforementioned regulatory act will be replaced by Law No. 195/2024 on the protection of personal data, which will repeat a number of legal requirements from the previous regulatory act, and will supplement it with new legal requirements.

In this regard, we list below the legal requirements found in Law no. 133/2011 but also which will be found in Law no. 195/2024 which are enforceable against political parties and the CEC.

In accordance with the provisions of Law no. 133/2011, political parties are personal data controllers, who process personal data relating to party members, party supporters, donors and dividend payers. Given these considerations, the legal framework obliges political parties and the CEC to the following activities:

I. **To designate a person responsible for data protection (DPO)** – Political parties and the CEC are obliged to designate a person responsible for data protection. In accordance with the provisions of art. 25 of Law no. 133/2011 on the protection of personal data, the tasks of the person responsible for the protection of personal data may be performed by:
   - The designated employee; or
   - Natural/legal person under a service contract.

Criteria for selecting the responsible person: In accordance with the provisions of art. 25 paragraph (4) of Law no. 133/2011 on the protection of personal data, the person responsible for data protection must have:

- Specialized theoretical knowledge (in the legal field, information technologies and the company's field of activity);
- Practical specialized knowledge (in the legal field, information technologies and the company's field of activity);
- Must have the capabilities to perform the responsibilities of the data protection officer.

Responsibilities of the data protection officer:

- Informs and provides advice to the operator and/or persons empowered by the operator, as well as to employees in activities related to the processing of personal data, compliance with the Personal Data Protection Policy and the legal framework in the field of personal data protection, including the allocation of responsibilities and awareness-raising and training actions for personnel involved in processing operations, as well as related audits;
- Informs and explains the rights of personal data subjects;
- Advises on the requirements of the legislation on the protection of personal data when examining requests, complaints, notifications, claims submitted in the context of the field of personal data protection;
- Approves proposals, regulations, instructions, standard acts that regulate/establish the processing and protection of personal data;
- Upon request, advises on the assessment of the impact on the protection of personal data;
- Represents the operator on issues related to the field of personal data protection;
- Informs the operator, the persons authorized by the operator and their employees about trends and changes in the field of personal data protection, and proposes the necessary changes;
- Cooperates with the National Center for Personal Data Protection, including as a contact point in case of prior consultation with it;
- Represents the data controller in relation to the National Center for Personal Data Protection, as well as other public authorities or private entities in relation to the legal regime of personal data protection;
- Performs other tasks established in agreement with the data controller provided that none of these tasks and duties generate a conflict of interest.

Mode of subordination and interaction with the person responsible for data protection:

- The person responsible for data protection must have direct subordination to the highest level of management Administrator/Executive Committee/Council (in accordance with the provisions of art. 25/1 paragraph (3) of Law no. 133/2011 on the protection of personal data);
- The operator (political parties, CEC):
    - must appropriately involve the DPO in all aspects related to the protection of personal data;
    - provides support to the DPO in carrying out his/her tasks and responsibilities;
    - provides support for training, maintaining and updating their specialist knowledge;
    - provides access to personal data and personal data processing operations;
    - the contact details of the DPO must be displayed for public access to employees/customers/visitors on all available resources (website/at the headquarters, etc.), and must be notified to the CNPDCP;
    - the DPO cannot be sanctioned or dismissed for performing his/her duties.

II. To conduct a Data Protection Impact Assessment – Political parties and the CEC are required to carry out a data protection impact assessment in the following cases (Law No. 133/2011 and Law No. 195/2024):

- Systematic and comprehensive evaluation of personal aspects based on automated processing, including profiling, that forms the basis for automated decisions with legal or similarly significant effects;
- Large-scale processing of special categories of data (racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, data concerning sex life or sexual orientation, criminal convictions and offences)
- Systematic, large-scale monitoring of a publicly accessible area.

For political parties specifically, a data protection impact assessment is indicated for the following processes (art. 23 of Law No. 133/2011; art. 35 of Law No. 195/2024):

- Records of party members;

- Video surveillance;
- Website functionalities: cookies, newsletter, donation of funds;
- Interaction with supporters.

The impact assessment must contain the following elements:

1. The identity, capacity and specific characteristics of the personal data controller (and, where applicable, persons empowered by the controller);
2. Purpose of processing personal data;
3. Volume, categories of personal data and type of data;
4. Type of personal data subjects;
5. Legal basis for processing personal data;
6. Traceability of personal data, including: (a) data collection method; (b) how data is stored and used; (c) the full processing cycle (organizing, storing, preserving, restoring, adapting, extracting, consulting, using, disclosing, transmitting, disseminating, joining, combining, blocking, erasing or destroying);
7. Assessment of the necessity and proportionality of processing operations in relation to the purposes;
8. Assessment of the risks to the rights and freedoms of the data subject;
9. How data subjects may exercise their rights;
10. Organizational and technical procedures to reduce the risks of security incidents;
11. Risks identified for compliance with personal data protection requirements;
12. Measures to remediate identified risks;
13. Data Protection Officer's opinion;
14. Conclusions;
15. Approval by the operator.

III. **To follow general data protection obligations** – under Law No. 133/2011 (and Law No. 195/2024 from 23 August 2026), political parties as data controllers have a number of other obligations.

5. Liability for violation of personal data protection requirements (unofficial translation)

In accordance with the applicable legal framework, the liability is provided for violation of the provisions of the legislation on the protection of personal data is described below.

Misdemeanor Code – The following violations are subject to fines:

- Failure to comply with basic conditions for processing, storage and use of personal data: fine of 60-90 conventional units (individual), 90–180 conventional units (person in a responsible position), 120–300 conventional units (legal entity), with possible deprivation of the right to carry out a certain activity for 3 months to 1 year;
- Violation of the rights of personal data subjects (to be informed, to access data, to intervene, to object, not to be subject to an individual decision): same scale of fines and possible deprivation of activity rights;
- Cross-border transmission of personal data in violation of data protection legislation: same scale of fines and possible deprivation of activity rights.

Criminal Code – Article 177 (Violation of the Inviolability of Personal Life)

- Illegal collection or dissemination of information protected by law about a person's private life without consent: fine up to 650 conventional units or 180-240 hours of unpaid community service;
- Illegal collection using special technical means: fine of 550-750 conventional units or 200–240 hours of unpaid community service;
- Dissemination in public discourse, through the media, using a position of office, or for reasons of prejudice: fine of 550-850 conventional units or deprivation of the right to hold certain positions

for 1 year, or 180-240 hours of unpaid community service; fine applied to legal entity of 2,000-3,000 conventional units;

- Dissemination of sexual content for purposes of revenge, hatred, humiliation or harm: fine of 550-850 conventional units, or 180-240 hours of unpaid community service, or imprisonment of up to 2 years.

Civil Code – Article 43 (Personality Rights) – Every natural person has inalienable and non-transferable rights to life, health, physical and mental integrity, free expression, name, honor, dignity, professional reputation, one's own image, respect for intimate, family and private life, protection of personal data, and other such rights recognized by law.

Law No. 195/2024 on the Protection of Personal Data – Provides for administrative sanctions of up to 2 million MDL or 2% of the total income obtained in the previous year.

Notably, under Law No. 195/2024 on the protection of personal data, the following sanctions could be applied regarding the activities of the political parties and the CEC, including other actors involved in the processing of personal data.

Sanctions of up to 1 million MDL or up to 1% of turnover, for the following acts:

a) Processing data where it no longer requires the identification of the person (art. 11);
b) privacy requirements by default and privacy by design (art. 25;
c) Lack of record keeping of personal data processing activities (art. 30);
d) Lack of cooperation with the CNPDCP (art. 31);
e) Lack of adequate security measures in data processing (art. 32);
f) Failure to notify the CNPDCP of cases of violation of Law No. 195/2024 (art. 33);
g) Failure to inform data subjects about the occurrence of security breaches (art. 34);
h) Failure to carry out a data protection impact assessment (art. 35);
i) Failure to carry out prior consultation with the CNPDCP in case of identification of high risks (art. 36);
j) Violation of the requirements towards the data protection officer (art. 37-39):
   - Failure to designate the responsible person;
   - Lack of adequate qualifications for the person responsible;
   - The existence of conflicts of interest in the exercise of the duties of the responsible person;
   - Non-involvement of the responsible person in data processing activities and the protection measures provided;
   - Failure to display the identification data of the responsible person on the web page and failure to send them to the CNPDCP;
   - Failure to provide the responsible person with necessary resources (time, human resources, access, maintaining and increasing specialized knowledge);

Sanctions of up to 2 million MDL or up to 2% of turnover, for the following acts:

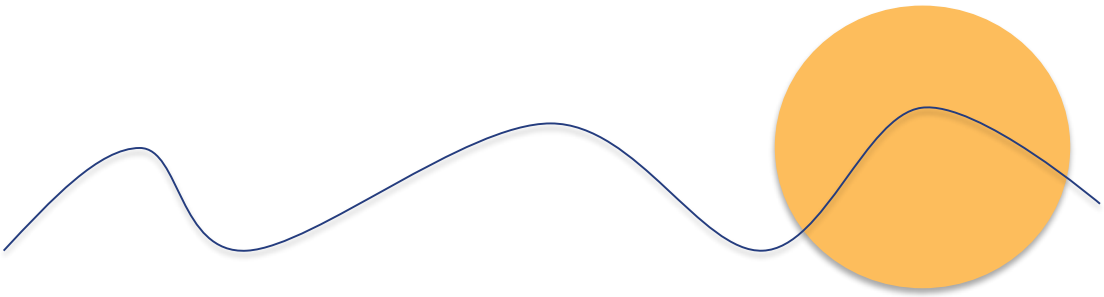
a) Data processed: illegally, excessively, in the absence of determined purposes, not updated, stored beyond the deadline, in the absence of adequate security measures (art. 5);
b) Data processed in the absence of a valid legal basis: consent, contract, legal obligation, protection of life and health of the person, performance of tasks in the public interest, legitimate interest (art. 6);
c) Data processing based on invalid or flawed consent (art. 7);
d) Processing of special categories of data in the absence of a valid legal basis (art. 9);
e) Failure to respect the rights of the data subject by violating:
   - Transparency requirements (art. 12);
   - Failure to provide information in case of collection of data from the data subject (art. 13);
   - Failure to provide information in the event that the data were not collected from the data subject (art. 14);
   - Violation of the right of access to data (art. 15);
   - Violation of the right to data rectification (art. 16);
   - Violation of the right to erasure of data (art. 17);
   - Violation of the right to restriction of processing (art. 18);
   - Violation of the notification obligation regarding the rectification or deletion of data (art. 19);

- Violation of the right to data portability (art. 20);
- Violation of the right to object (art. 21);
- Violation of the right to automated decision-making and profiling (art. 22);

f) Transmission of data in violation of the requirements regarding:
- cross-border transfer (art. 44-46);
- in violation of mandatory corporate rules (Art. 47);
- unauthorized disclosures established by regulatory acts (Art. 48).

Annex 2: List of analyzed websites

Parliamentary party	Web page
Partidul Acţiune şi Solidaritate / Party of Action and Solidarity	https://www.unpaspentru.md/
Partidul Socialiştilor din Republica Moldova / Party of Socialists of the Republic of Moldova	https://socialistii.md/
Partidul Nostru / Our Party	https://www.partidulnostru.md/
Partidul Democraţia Acasă / Democracy at Home Party	https://pda.md/
Partidul Comunistilor din Republica Moldova / Party of Communists of the Republic of Moldova	https://www.pcrm.md/md/
Partidul „Mişcarea Alternativa Naţională" / National Alternative Movement Party	https://alternativa.eu/
Partidul Dezvoltării şi Consolidării Moldovei / Party for the Development and Consolidation of Moldova	https://pdcm.md/
Congresul Civic / Civic Congress	https://congresulcivic.md/md/
Partidul Viitorul Moldovei / Future of Moldova Party	https://viitorulmoldovei.md/ro/acasa/



Annex 3: Assessment questions for political parties (RO)

1. Ce categorii de date cu caracter personal prelucrează partidul politic în cadrul activităţilor sale de campanie?
2. Vă rugăm să enumeraţi toate modalităţile prin care partidul poate colecta astfel de date (de exemplu, în timpul campaniei electorale din uşă în uşă, chestionarea în stradă, la evenimente politice,...)
3. Aveţi acces şi colectaţi date prin intermediul registrelor de stat?
4. În momentul colectării datelor de la persoanele fizice, sunt comunicate scopurile în care vor fi prelucrate date?
5. Li se oferă persoanelor vizate posibilitatea de a-şi da consimţământul explicit înainte ca datele să fie colectate?
6. Datele colectate sunt prelucrate în baza unui proces decizional automatizat, inclusiv dacă se crează profile ale persoanelor fizice?
7. Are partidul o politică internă de protecţie a datelor?
8. Dacă da, a fost pus la dispoziţia publicului la sedii sau prin pagina web/resursele social media?
9. Partidul duce evidenţa activităţilor (fluxurilor) de prelucrare a datelor cu caracter personal?
10. Partidul a efectuat o evaluare a Impactului asupra Protecţiei Datelor?
11. Partidul a desemnat o persoană responsabilă de protecţia datelor cu caracter personal?
12. Dacă da, sunt publicate informaţiile de contact ale responsabilului cu protecţia datelor?
13. Au existat incidente de securitate pe domeniul protecţiei datelor în ultimii 5 ani? Dacă da, vă rugăm să descrieţi.
14. Partidul trimite e-mailuri sau mesaje SMS cu conţinut promoţional? Dacă da, a obţinut consimţământul prealabil al destinatarilor?
15. Dacă partidul contactează alegătorii prin telefon sau poştă, li se oferă informaţii clare despre dreptul lor de a refuza?
16. Este opţiunea de dezabonare inclusă în fiecare comunicare cu persoanele fizice?
17. Cum se asigură partidul că obiecţiile/refuzurile din partea persoanelor fizice sunt respectate?
18. Dacă partidul desfăşoară comunicare prin grupuri de mesagerie (Whatsapp, Viber, Telegram etc.) – se obţine consimţământul fiecărei persoane înainte de adăugarea sa?
19. Dacă partidul utilizează centre de apel sau trimiteri masive de SMS-uri – acest proces este realizat de persoane autorizate?
20. Dacă da, ce statut au aceste persoane? Sunt încheiate contracte sau alte forme de implicare?
21. Dacă datele sunt transferate în afara Moldovei şi în afara UE, sunt implementate măsuri de siguranţă privind protecţia datelor?
22. Partidul distribuie date cu caracter personal ale alegătorilor unor terţe părţi?
23. Dacă da, sunt alegătorii/persoanele vizate informate? Cum?
24. Dacă da, există contracte sau acorduri cu terţe părţi?
25. Are partidul implementat proceduri pentru a se asigura că datele personale ale alegătorilor sunt corecte şi actualizate?
26. Cum asigură partidul confidenţialitatea, integritatea şi disponibilitatea datelor cu caracter personal?
27. Partidul îşi instruieşte personalul care prelucrează date cu caracter personal cu privire la cerinţele de protecţie a datelor?
28. Au existat controale/verificări ale partidului de către Centrul Naţional pentru Protecţia Datelor cu Caracter Personal în ultimii 5 ani?
29. Au fost instruiţi reprezentanţii relevanţi ai partidului de către CNPDCP sau Comisia Electorală Centrală?
30. Partidul este mulţumit de interacţiunea cu CNPDCP şi CEC, precum şi de acţiunile întreprinse de aceste autorităţi?
31. Aveţi sugestii sau propuneri privind îmbunătăţirea cadrului legal sau a măsurilor de protecţie a datelor?
32. Vă rugăm să transmiteţi link-ul către Politica de protecţie a datelor cu caracter personal a partidului.

Annex 4: Assessment questions for the CEC (RO)

Întrebări generale:

1. A efectuat CEC o evaluare a impactului asupra protecţiei datelor (art. 23 din Legea nr. 133/2011)?
2. A numit CEC un responsabil cu protecţia datelor (art. 25 din Legea nr. 133/2011)?
3. Sunt informaţiile de contact ale responsabilului cu protecţia datelor publicate pe site-ul web şi la Autoritatea pentru Protecţia Datelor cu Caracter Personal (CNPDCP) ?
4. Are CEC o Politică internă de protecţie a datelor? Dacă da, vă rugăm să indicaţi în ce an a fost aprobată, de câte ori a fost modificată (în ce an), pe ce cadru legal se bazează şi ce module/capitole are?
5. Când informaţiile despre deciziile CEC sunt publicate online, cum asigură CEC respectarea reglementărilor privind protecţia datelor cu caracter personal?
6. A cooperat CEC cu Autoritatea pentru Protecţia Datelor cu Caracter Personal (CNPDCP) în ceea ce priveşte îmbunătăţirea protecţiei datelor cu caracter personal ale cetăţenilor moldoveni în timpul alegerilor?
7. A efectuat CEC o consultare prealabilă cu CNPDCP în conformitate cu art. 24 din Legea nr. 133/2011?
8. A primit CEC plângeri privind gestionarea abuzivă a datelor cu caracter personal, inclusiv în cazul transferurilor transfrontaliere de date ale subiecţilor electorali, în ultimii 5 ani? Dacă da, care au fost acestea şi ce măsuri au fost întreprinse ?
9. A oferit CEC instruire sau îndrumări scrise alegătorilor, partidelor politice/candidaţilor sau altor subiecţi ai procesului electoral cu privire la protecţia datelor cu caracter personal în timpul alegerilor?
10. Transferă CEC date cu caracter personal în afara graniţelor Republicii Moldova către ţări care NU asigură un nivel adecvat de protecţie a datelor? Dacă da, vă rugăm să indicaţi aceste ţări şi ce măsuri de protecţie a datelor au fost luate de CEC.
11. Aveţi recomandări privind îmbunătăţirea protecţiei datelor cu caracter personal ale cetăţenilor moldoveni în timpul procesului electoral?

Înregistrarea alegătorilor şi votul

12. Este accesul la Registrul de Stat al Alegătorilor (RSA) limitat în mod corespunzător?
13. Cine are acces la RSA şi există o procedură internă care reglementează accesul?
14. Cum se asigură CEC că alegătorii îşi pot verifica doar propriile date personale?
15. Au fost publicate listele electorale de către CEC pe site-ul său oficial în anii precedenţi? Dacă da, vă rugăm să indicaţi perioada şi justificarea juridică pentru aceasta.
16. A publicat anterior CEC corespondenţa primită şi trimisă pe site-ul său web, inclusiv date despre alegători şi membri de partid? Dacă da, vă rugăm să ne furnizaţi perioada de timp în care datele au fost accesibile şi temeiul legal pentru publicare.
17. Ce informaţii despre alegători sunt publicate în prezent sau disponibile la cerere?
18. Există termeni de stocare şi perioade de păstrare diferite pentru diferite categorii de date? Dacă da, vă rugăm să ne spuneţi în ce documente sunt furnizate şi de unde pot fi accesate.
19. Cum sunt obţinute informaţiile din RSA de la Agenţia Serviciilor Publice, prin Mconnect, SIC Acces Web sau prin alte metode? Vă rugăm să le specificaţi.
20. Când alegătorii şi membrii de partid sunt informaţi de către CEC că datele lor sunt prelucrate, au alegătorii posibilitatea de a vizualiza în Mconnect sau SIC Acces Web faptul prelucrării datelor de către CEC?
21. Cum se asigură CEC că prelucrează doar datele necesare pentru înregistrarea alegătorilor RSA? Ce categorii de date cu caracter personal sunt prelucrate?
22. Consumă CEC date prin Mconnect ? Dacă da, vă rugăm să descrieţi care sunt fluxurile şi categoriile de date.
23. Sunt specificate în mod clar scopurile pentru care sunt prelucrate datele cu caracter personal? Unde?
24. Cum se asigură CEC că datele RSA sunt utilizate doar în scopuri electorale specificate?

25. A implementat CEC măsuri tehnice şi organizatorice adecvate pentru securitatea datelor electorale? Care sunt acestea?
26. Are CEC proceduri pentru notificarea încălcărilor către autoritatea de supraveghere şi către persoanele vizate afectate?
27. Au existat incidente care ar fi putut compromite securitatea sau integritatea RSA sau a altor date electorale în ultimii 5 ani? Vă rugăm să le descrieţi.
28. Au existat tentative de acces neautorizat sau manipulare a datelor RSA / listelor electorale în ultimii 5 ani? Vă rugăm să le descrieţi. Au fost luate măsuri în urma acţiunilor ulterioare?
29. Primesc membrii comisiei electorale care se ocupă de RSA instruire în domeniul securităţii informaţiilor?

Înregistrarea candidaţilor şi finanţarea partidelor

30. Ce date despre candidaţi sunt disponibile publicului şi trebuie publicate, comparativ cu ce date despre candidaţi sunt utilizate doar de persoanele care ocupă poziţii autoritare?
31. Ce date despre donatorii partidelor politice sunt disponibile publicului faţă de ce date sunt utilizate doar de persoanele care ocupă poziţii autoritare?
32. Atunci când informaţiile privind situaţia financiară a candidaţilor, rapoartele financiare ale partidelor politice şi donaţiile sunt furnizate cetăţenilor la cerere sau publicate online, cum asigură CEC respectarea reglementărilor privind protecţia datelor cu caracter personal?
33. Supraveghere video la secţiile de votare?
34. A fost efectuată o Evaluare a Impactului asupra Protecţiei Datelor pentru procesul de supraveghere video utilizat de CEC pentru a supraveghea secţiile de votare?

Annex 5: Questions for the CNPDCP (RO)

1. Câte plângeri în ultimii 5 ani au fost depuse pe partidele politice sau CEC în legătură cu prelucrarea neconformă a datelor, cu specificare în câte cazuri s-a dat curs (s-a efectuat controlul) în câte cazuri plângere au fost examinate ca petiţii (fără efectuarea controlului) şi ce măsuri au fost dispuse?
2. Câte cazuri de autosesizare şi efectuare a controlului au fost realizate de CNPDCP în raport cu partidele politice, CEC sau alte entităţi care prelucrează datele alegătorilor, membrilor de partid şi altor persoane în domeniul electoral?
3. Au fost constatate cazuri de transmitere transfrontalieră neconformă a datelor cu caracter personal ale alegătorilor, membrilor de partid, în caz afirmativ vă rugăm să specificaţi tipurile de încălcări şi măsurile de constrângere aplicate?
4. În perioada ultimelor 5 ani, au fost elaborate Instrucţiuni sau recomandări în domeniu electoral, în caz afirmativ vă rugăm să le specificaţi?
5. Câte instruiri au fost realizate de CNPDCP în raport cu partidele politice şi CEC în ultimii 5 ani;
6. Câte dintre partidele politice, din Republica Moldova au informat CNPDCP cu privire la desemnarea unui responsabil cu protecţia datelor şi câte informări au fost efectuate la general (pe ţară) de către toţi operatorii de date?
7. Câte cazuri de consultări prealabile efectuate în ordinea prevăzută de art. 24 din Legea nr. 133/2011, au fost solicitate de partidele politice şi de CEC din 2022 – prezent?
8. În ultimii 5 ani au fost cazuri în care CNPDCP să pună în aplicare atribuţia prevăzută de art. 6 alin. (2) din Legea nr. 133/2011, prin intermediul căruia să interzică Partidelor politice sau altor entităţi de drept public sau privat de a prelucra categoriile speciale a datelor?
9. Ce măsuri a întreprins cu CNPDCP pentru a conforma prelucrarea datelor în domeniul electoral?
10. Au existat iniţiative de modificare a legislaţiei din partea CNPDCP pentru fortificarea dreptului la protecţia datelor în domeniul electoral?
11. Cadrul legal existent permite/asigură cu instrumentele necesare pentru exercitarea funcţiilor de control, supraveghere şi conformare a prelucrărilor de date din domeniul electoral de către CNPDCP?
12. Cum apreciază CNPDCP situaţia privind prelucrarea datelor în domeniul electoral şi care ar fi măsurile de întreprins pentru îmbunătăţirea situaţiei?

Promo-LEX Association
23/13 Mitropolit Petru Movila St.
Chisinau, Moldova
info@promolex.md / www.promolex.md