**  
  
The employees of more than 300 public institutions continue to use about 700 @mail.ru and @rambler.ru emails in 280 localities in 34 districts of Moldova. Quantitatively, 280 localities out of the total of 1400 attested in the RM, according to the 2014 census, would account for about 20 percent. This situation of negative impact, through multiple cyber risks for the state, contravenes not only the normative acts of the Ministry of Internal Affairs, but also the normative documents of the central state apparatus - the Presidency, the Parliament, the Government, the Ministry of Economic Development and Digitalization, the Ministry of Education, the Ministry of Foreign Affairs and European Integration, the Ministry of Finance and even the Ministry of Defence.**

The present investigation aims to understand the extent of the use of Russian e-mail resources (such as @mail.ru and @rambler.ru) by various public institutions in Moldova in the new geopolitical conjuncture, as well as the potential risks of using foreign digital resources.

**How we collected the data**

At the end of February 2024, we collected from open sources seven massive datasets using keywords in the Google Search search engine as follows:

A) "primary" AND "@mail.ru" site:.md

B) "примэрия" AND "@mail.ru" site:.md

C) "primaria" AND "@rambler.ru" site:.md

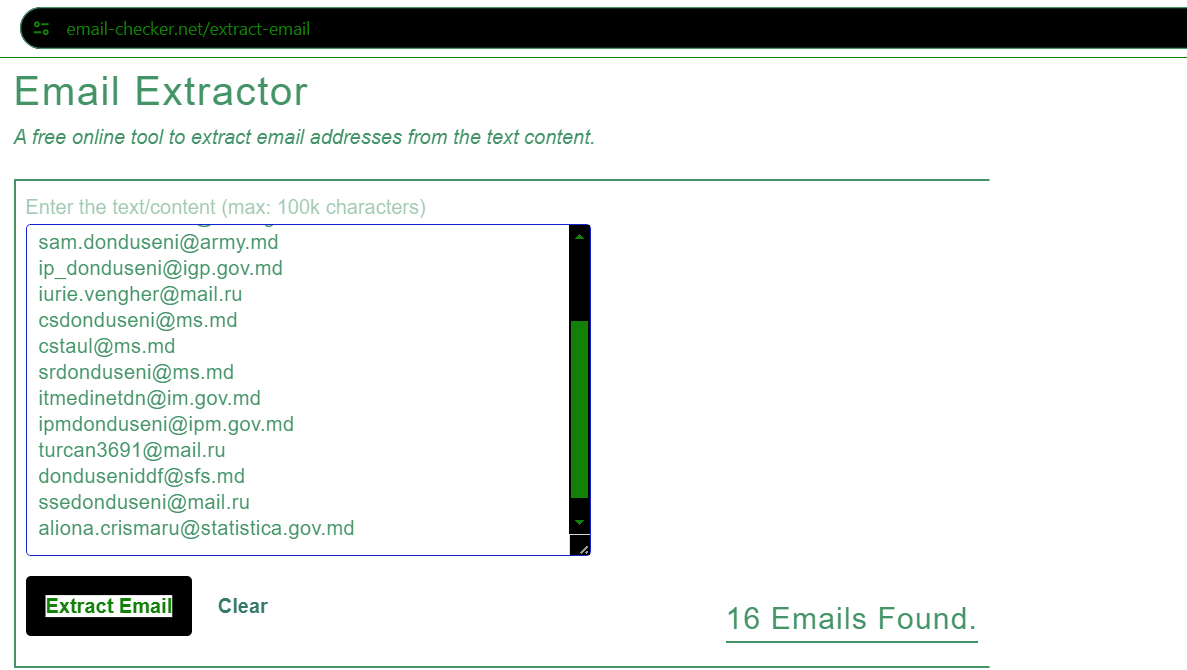
D) "примэрия" AND "@rambler.ru" site:.md

E) "minister" AND "@mail.ru" site:.md

F) "minister" AND "@rambler.ru" site:.md

G) "Public Services" AND "@mail.ru" site:.md

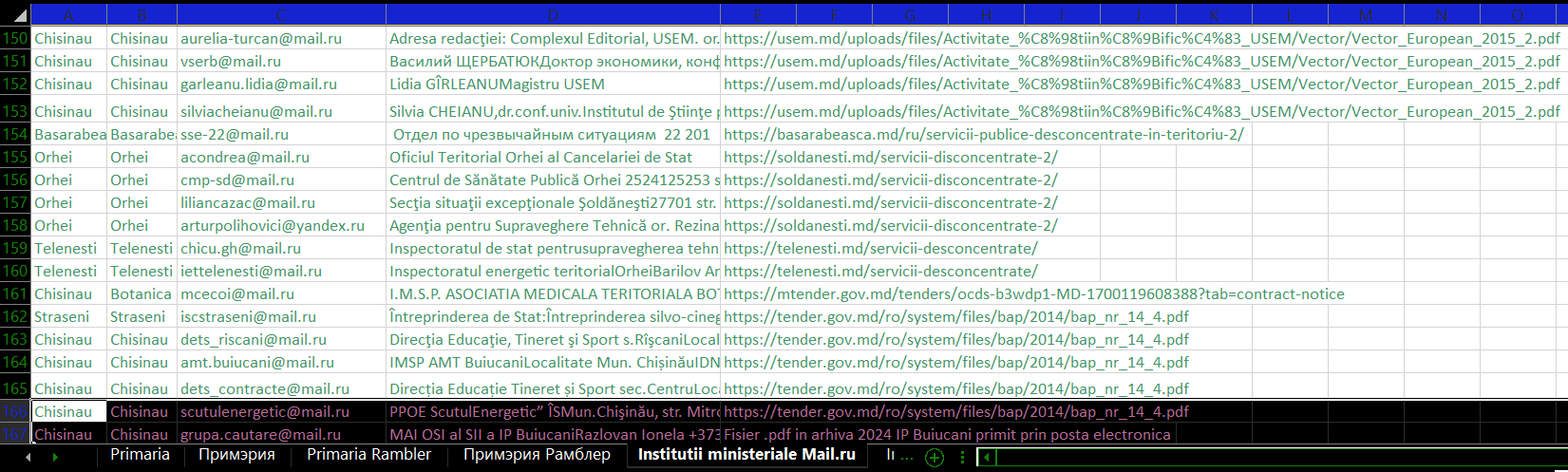
In most cases, the information identified in the Google results pages was extracted in bulk (unsorted, in text format) manually and by copying, and then, using specialized email capture programs (such as email-checker.net/extract-email), we obtained a "clean" list of emails easy to analyze.

  
**Photo source:** Actual browser screen. The interface of the free software for sorting emails from a massive text data, email-checker.net

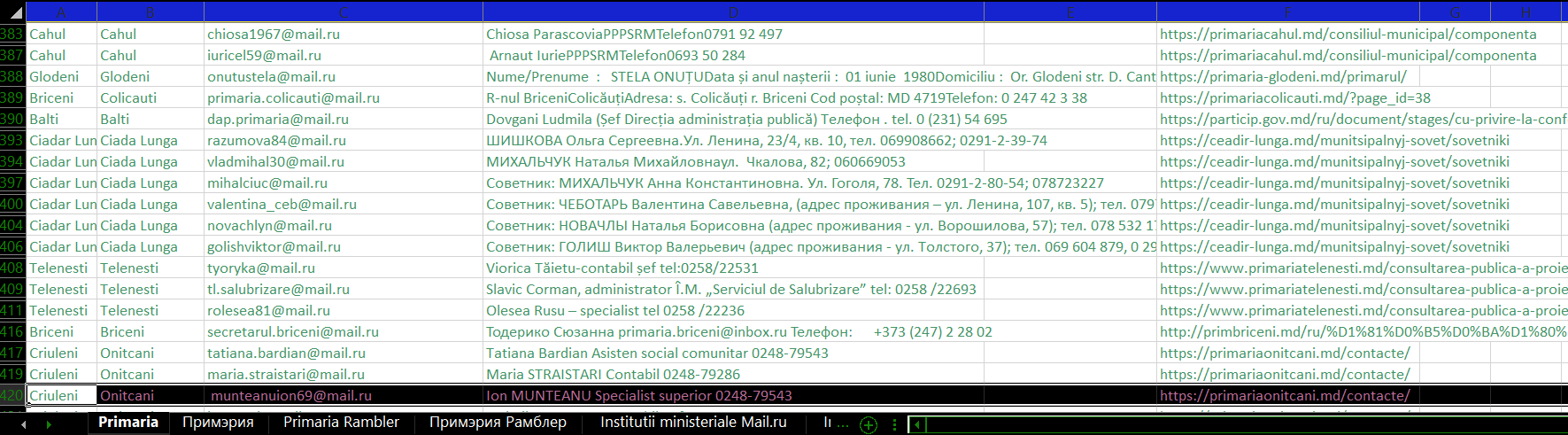
The unique e-mails thus obtained (about 900 in number) by semi-automatic selection and processing were structured according to the following reasoning: District - Locality - E-mail - Institution with contacts - Source of information and stored in a simple Excel file. \*[**The complete INDEX Search Database.xlsx file with the final formatted data identified can be downloaded here >>**](https://fbi.md/datas/users/1-index_search_database.xlsx)

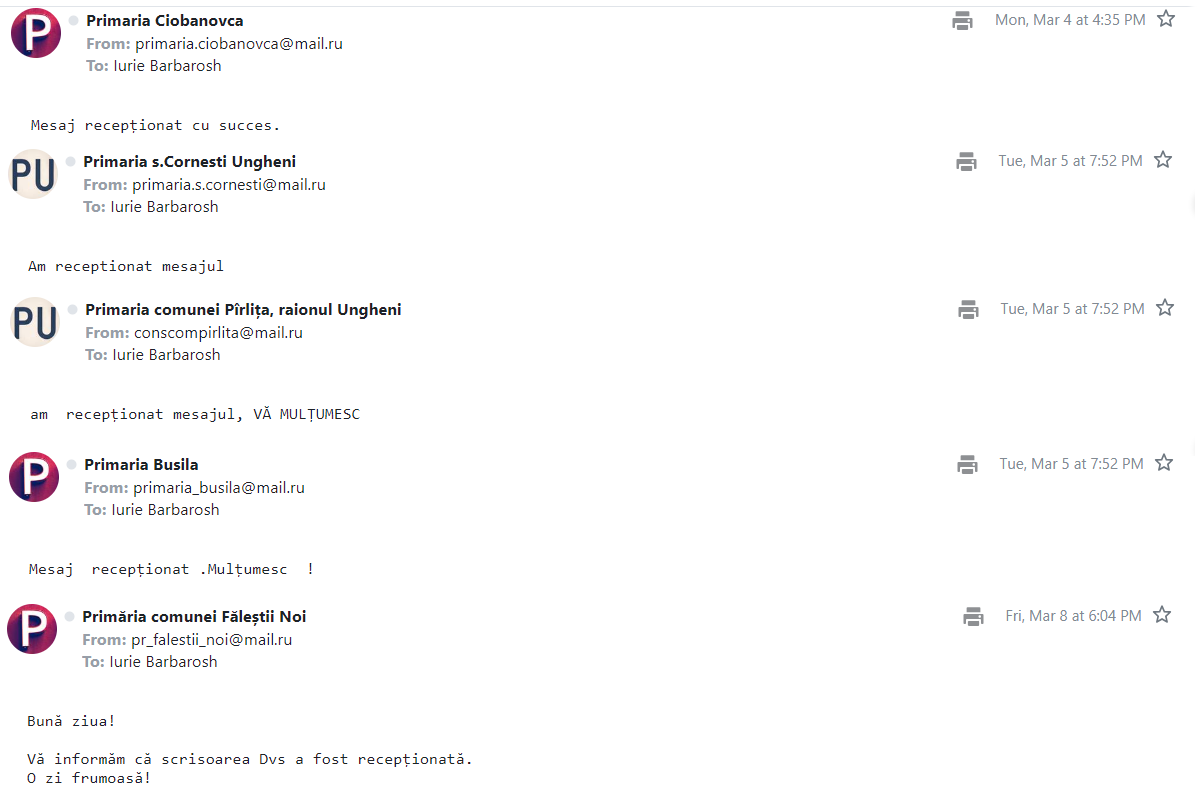
[**And the full Raw Archive with the .pdf reference pages of the collected information can be downloaded here (with a single compressed .zip file) >> >>**](https://drive.google.com/file/d/1mAJvYkMMDvIF1Z8s4yjp37b2gTv1OEUd/view?usp=sharing)

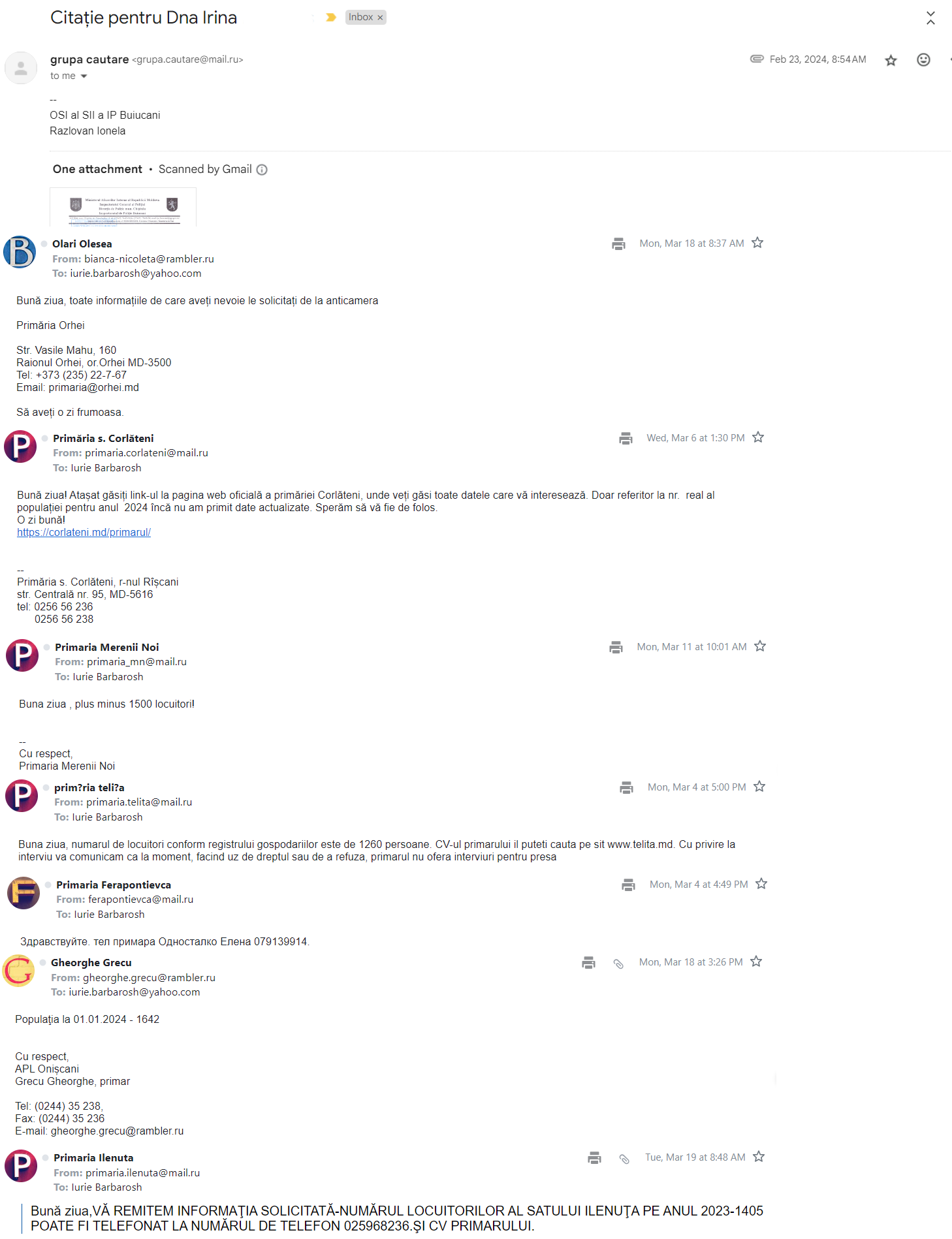
Thus, in addition to a list of hundreds of @mail.ru and @rambler.ru e-mails of city halls, district councils and various territorial agencies, we also find a list of institutions of the national health, education, research, finance and even defense system.

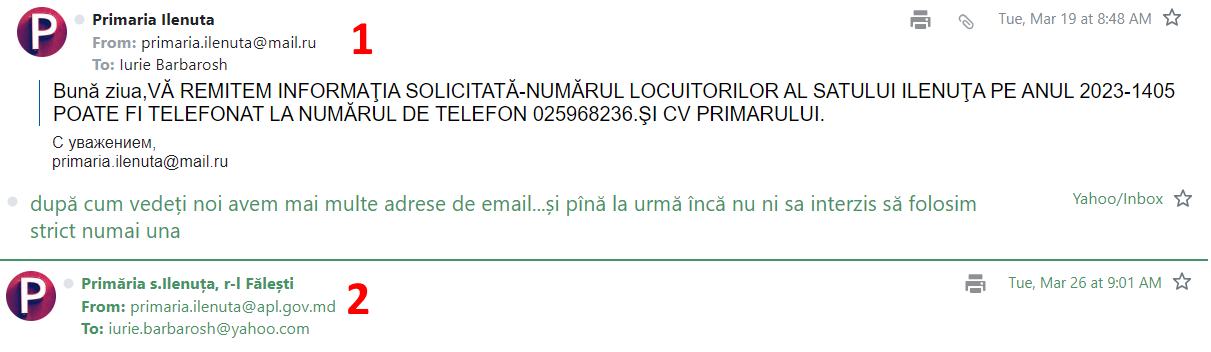


**Photo source:** Actual screen from Index Search Database.xlsx. Example list of ministerial level institutions in the Republic of Moldova that use @mail.ru e-mail in their work

We set out to understand how active these emails are, to date, of the municipalities and district councils of the Republic of Moldova...  
  
  
**Photo source:** Actual screen from Index Search Database.xlsx. Example list of local level institutions in the Republic of Moldova that use @mail.ru e-mail in their daily work

We have sent several messages to the identified addresses. In some cases, we received automated replies "Receipt" of the message:  
  
  
**Photo credit:** Real screen from the mailbox of investigative journalist Iurie Barbaroș. Automated responses received from the @mail.ru mailboxes of local public administration in Moldova.

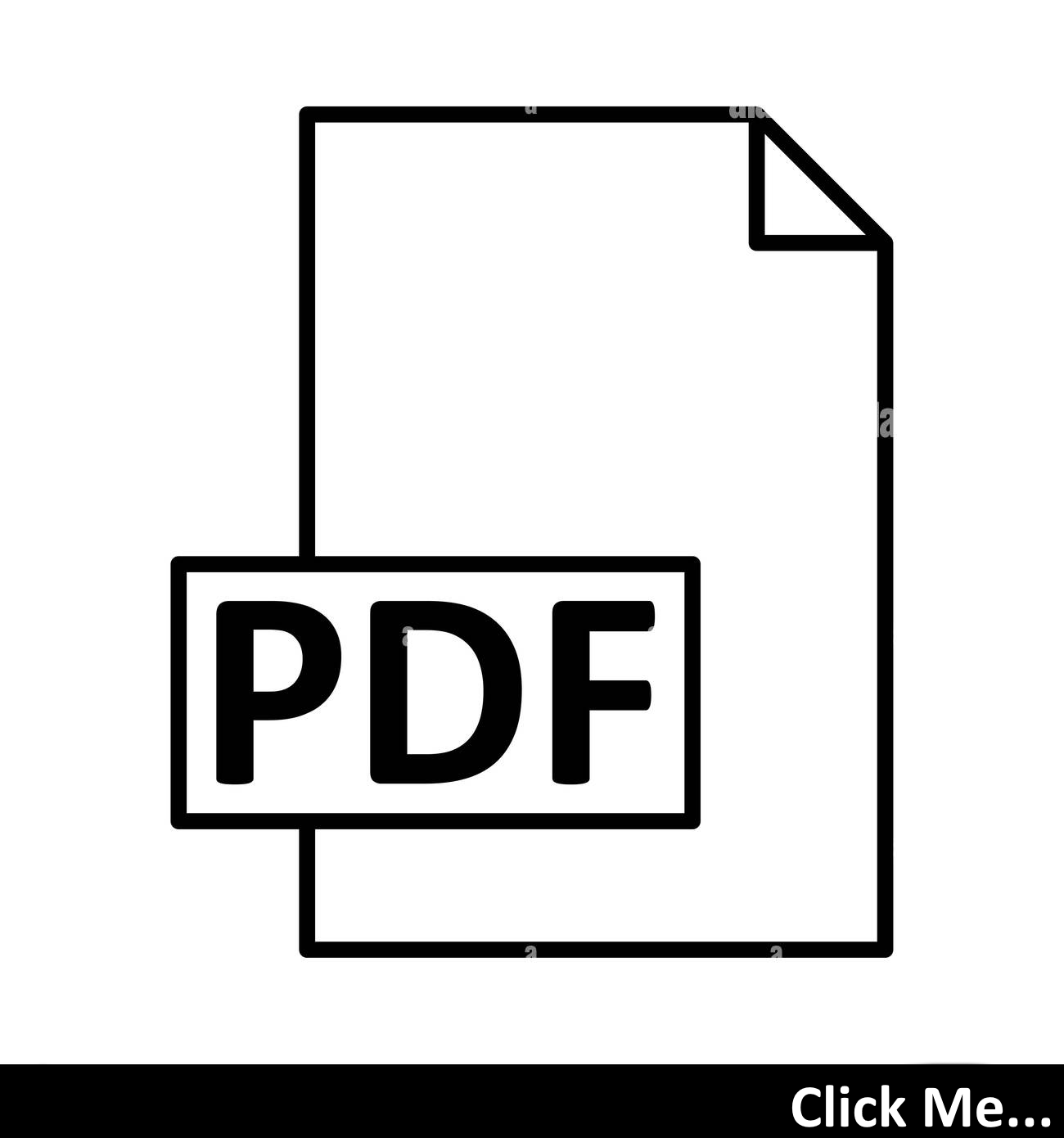
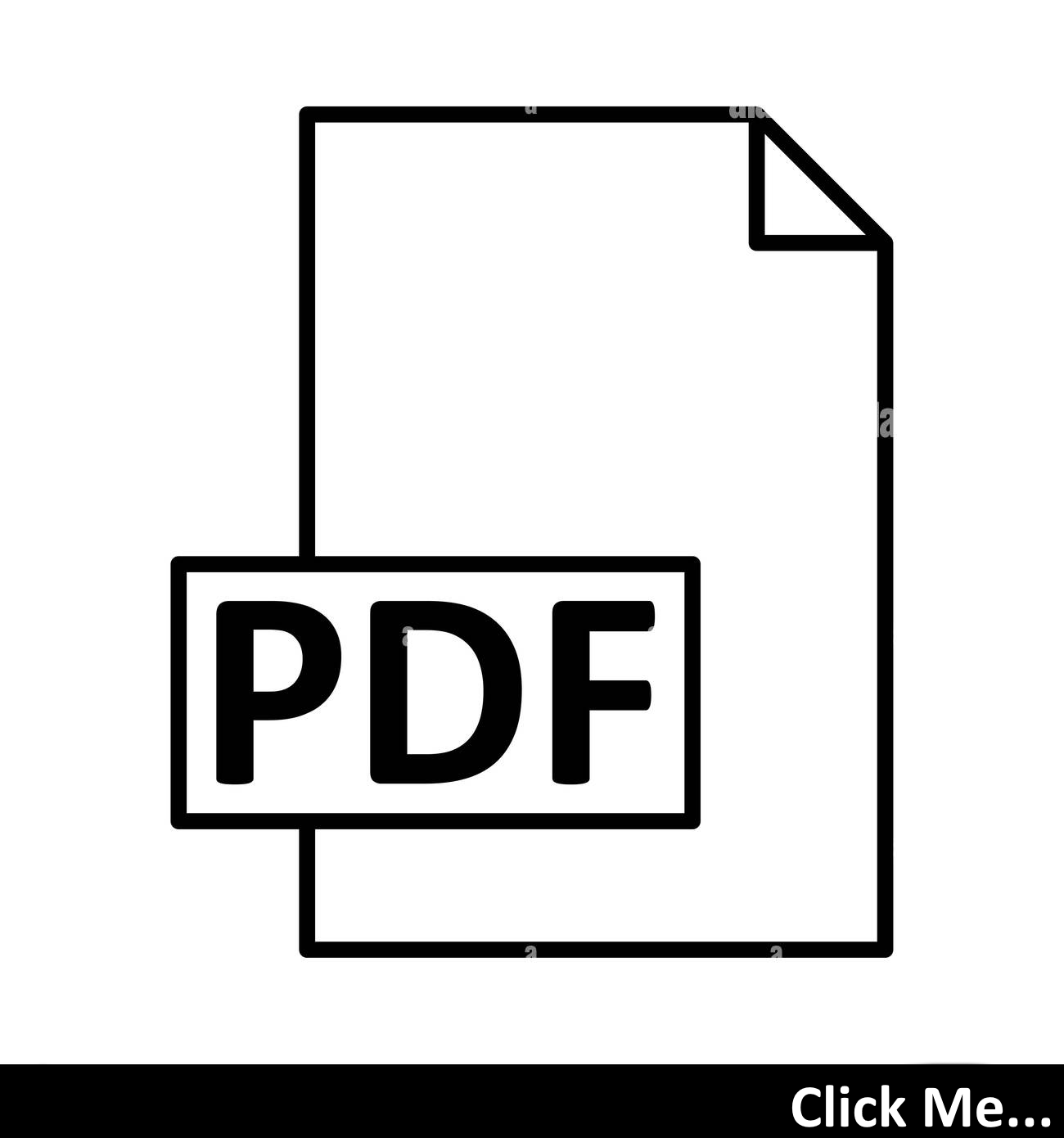
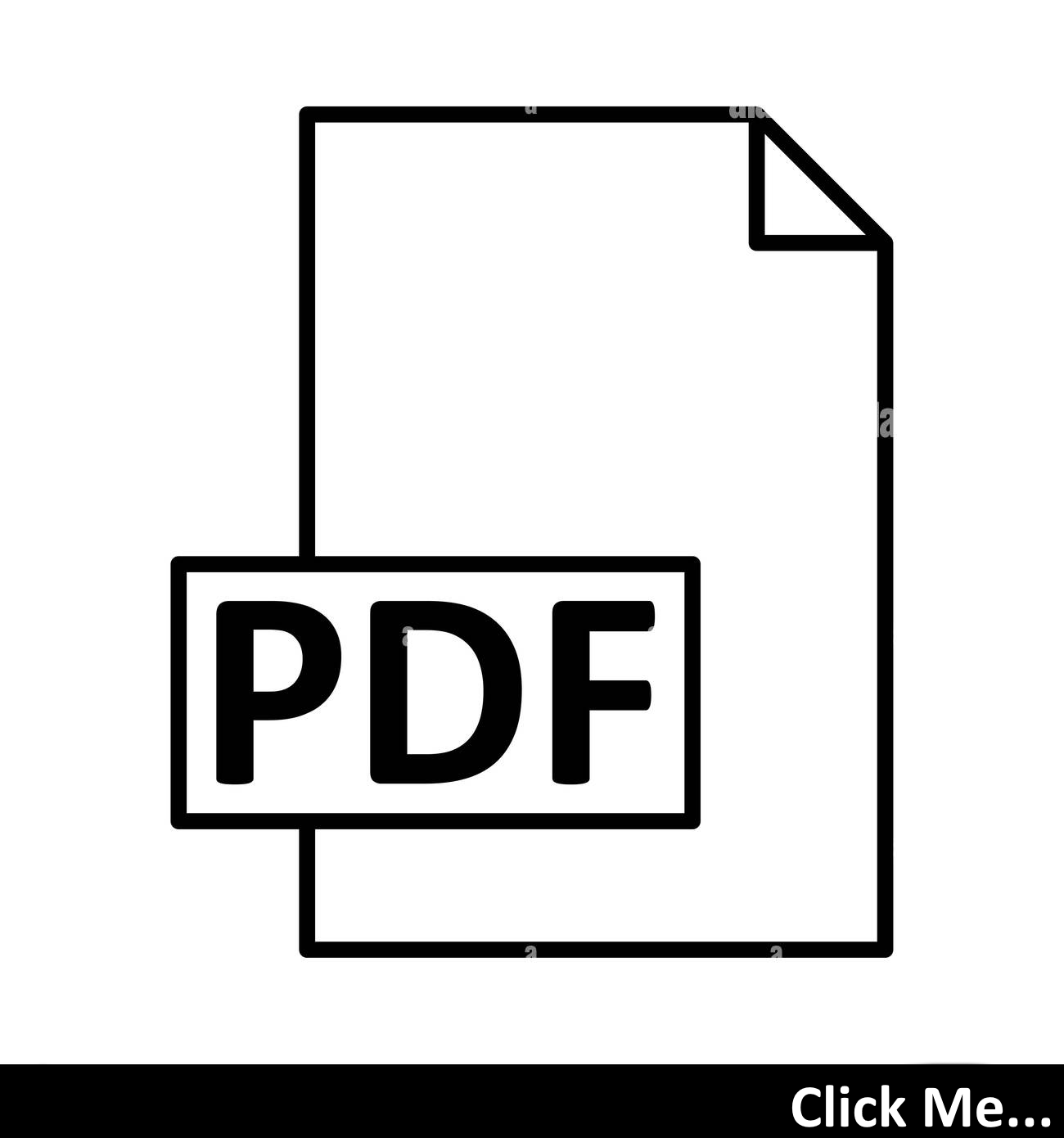
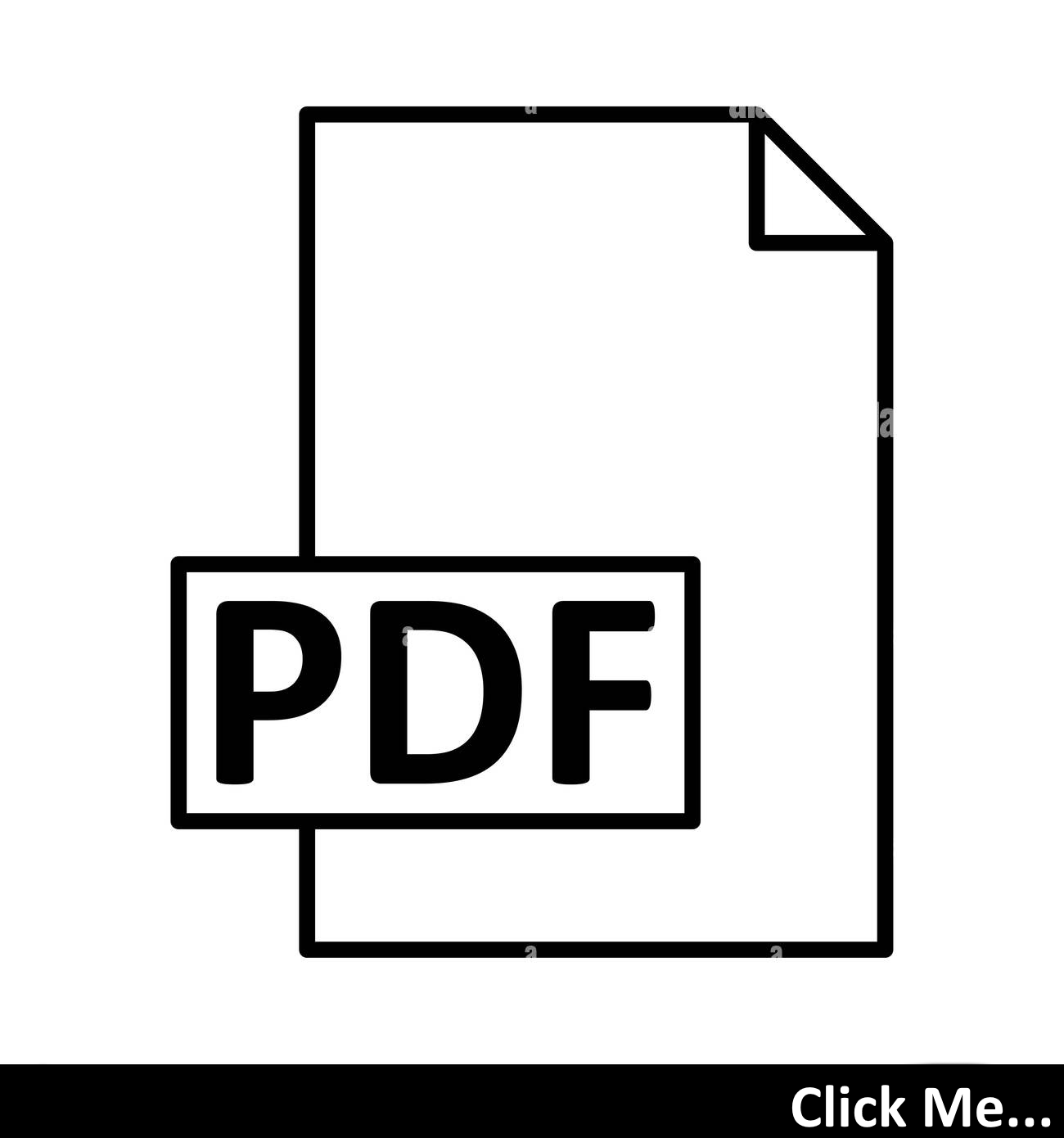
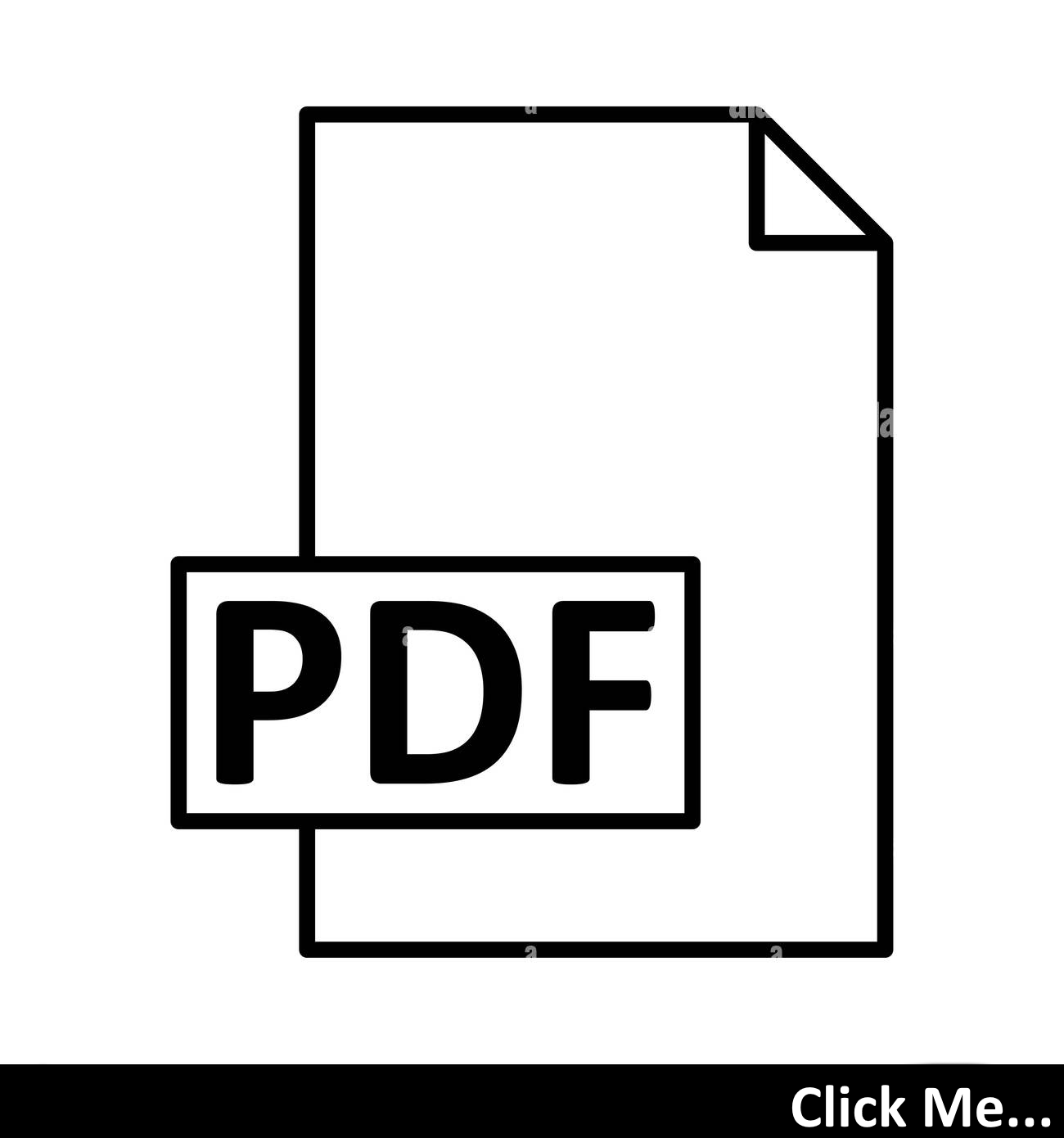
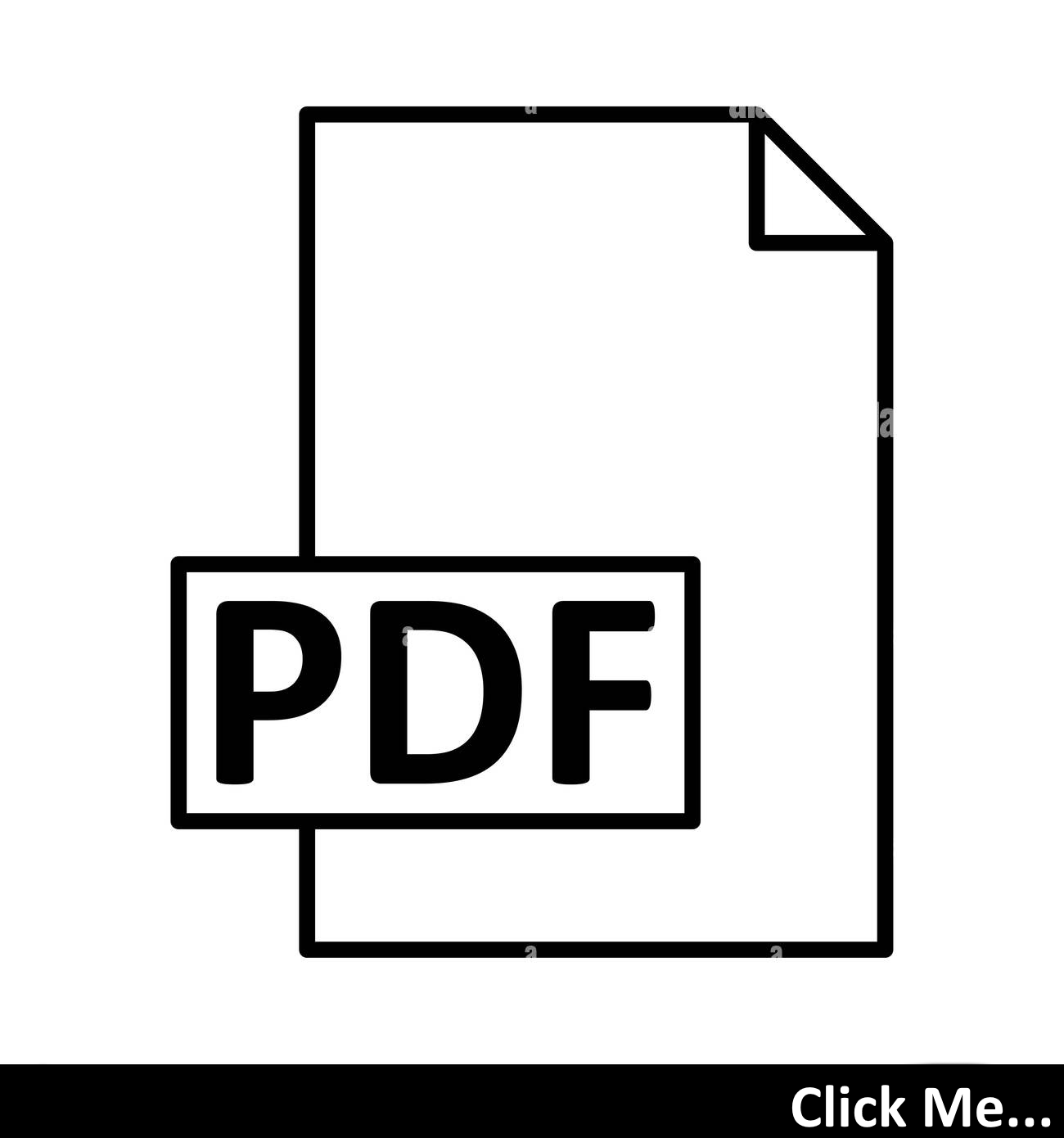
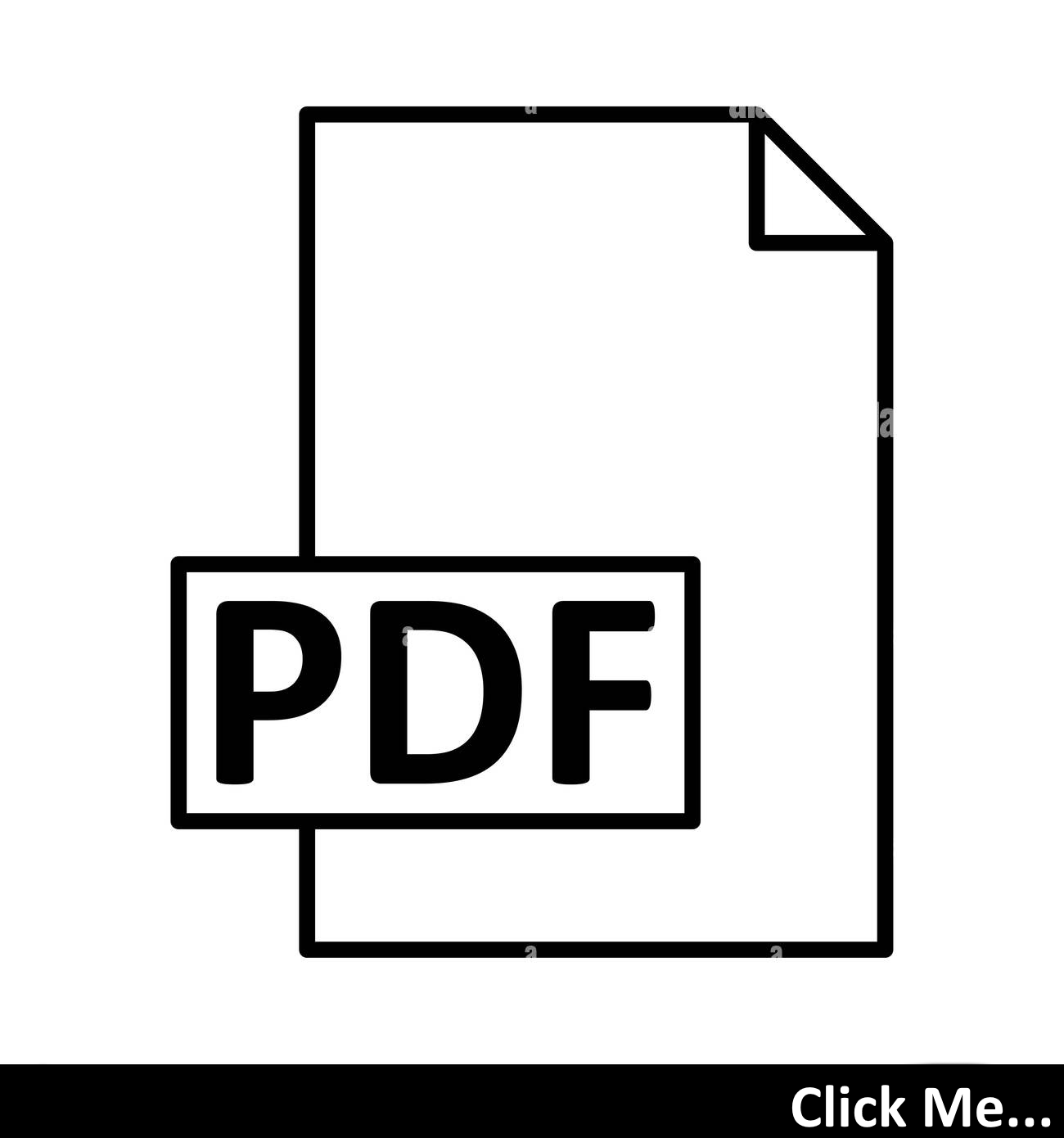
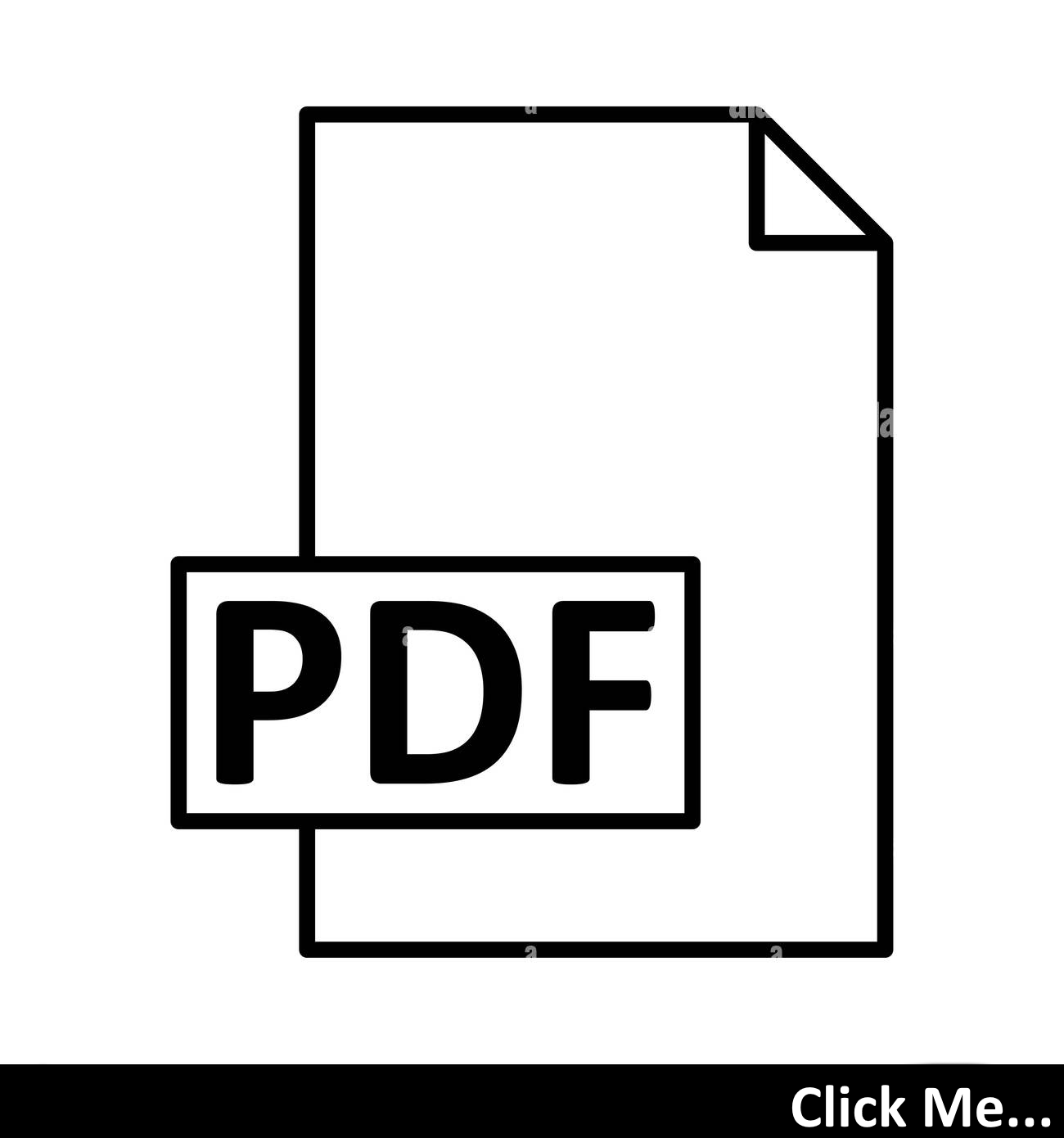
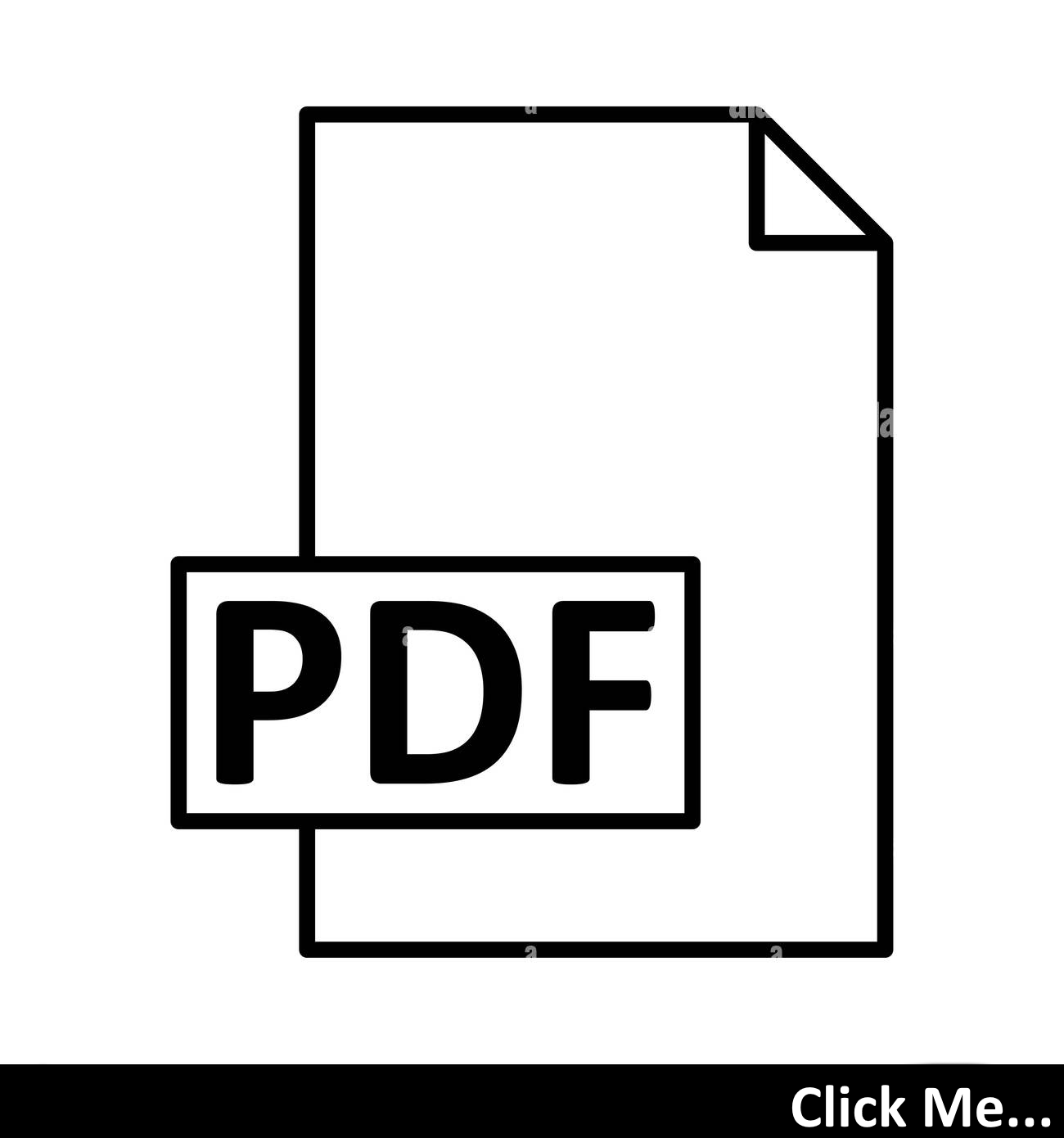
But in many other cases we received concrete answers, clearly involving the human factor, to our experimental questions:  
  
  
**Photo credit:** Real screen from the mailbox of investigative journalist Iurie Barbaroș. The logical and concluded answers received from the @mail.ru mailboxes of state institutions in the Republic of Moldova.

I asked several institutions from different districts why they opt for @mail.ru and @rambler.ru mailboxes instead of the national ones @mail.md or @apl.gov.md and I got only one answer (at the time of publication of this article) from the Ilenuța City Hall, in the Fălești district:  
  
  
**Photo credit:** Real screen from the mailbox of investigative journalist Iurie Barbaroș. Response by Mayor Gheorghe Grecu, s. Ilenuța, Fălești district.

Overall, this exercise demonstrated that at least some of the @mail.ru and @rambler.ru postal addresses are still actively in use, even if some e-mail addresses were collected from relatively old official tenderer pages, past the year 2020, or financial reports older than 2022.

**Legality and grounds for using @mail.ru and @rambler.ru services in public institutions**

With the intention to prove the legality of the use of @mail.ru and @rambler.ru addresses by local and central public administration institutions, we have sent several written requests to the authorized bodies of the Republic of Moldova. Among the recipient institutions were the Public Services Agency (they replied), the Ministry of Economic Development and Digitalization (they replied), the National Centre for Personal Data Protection (they replied twice), the Information Service of the Republic of Moldova, SIS (they replied), the Ministry of Energy (they replied), the Information Technology and Cyber Security Service, STISC (they replied) and the Information Technology Service of the Ministry of Interior (they replied), AO "Internet Community" (they replied).

Here are the replies we have received at the time of publication of this publication, pursuant to Law No. 133 of 08.07.2011 on the protection of personal data (art. 10), Law No. 148 of 09-06-2023 on access to information of public interest, Press Law No. 243 of 26.10.1994 and Law on freedom of expression No. 64 of 23.04.2010:  
  
[](https://fbi.md/datas/users/1-asp_nr.01-2956_din_19.03.2024.signed.pdf) [](https://fbi.md/datas/users/1-mded.pdf) [](https://fbi.md/datas/users/1-stisc.pdf) [](https://fbi.md/datas/users/1-sti_al_mai_rspuns_jurnalist_spe.signed.pdf)  [](https://fbi.md/datas/users/1-date_personale.pdf)  [](https://fbi.md/datas/users/1-riscuri_centru_date_cp_acces_la_informaii_2.signed.pdf) [](https://fbi.md/datas/users/1-ao_comunitatea_internet.pdf)  [](https://fbi.md/datas/users/1-sis-375.signed.pdf)  [](https://fbi.md/datas/users/1-ministerul_energiei_15-983_08.04.2024.pdf)  
**Legend**: Official responses in .pdf format, from left to right, ASP, MDED, STISC, STIMAI, CNPDCP (rules) and CNPDCP (risks), AO "Internet Community" (risks), SIS (risks), Ministry of Energy (statement).

In a relevant manner, the Information Technologies Service of the MAI specified in its reply that "the operator of the SPE (Electronic Mail Service) is the Public Institution "Information Technology and Cyber Security Service" (STISC), designated as the technical-technological operator of the public administration authorities (of all levels - ed.).

And the SPE is used in the interest of the service, for the transmission of information containing text messages, files, documents or correspondence, with the exception of classified information, provided for by the regulatory framework (Article 11 of Law No. 245/2008 on State Secrecy)". From which it follows that only STISC can be designated as the operator for local (town halls, local, district and territorial councils) and central public administration authorities, ministries and government agencies. All e-mails assigned by STISC with the ending .gov.md

**We find the same semantic charge in the response of the Information Technology and Cyber Security Service (STISC):**

"- in accordance with the provisions of Government Decision no. 822/2012, as well as the Order of the Secretary

General of the Government No. 67 of 7.06.2023 on the approval of the Regulation on the services

electronic mail system of the public administration authorities, STISC in its capacity as operator

technical-technological operator of the electronic mail system of public administration authorities provides

government entities with service mailboxes, created on the @gov.md sub-domain, ensuring a

high degree of information protection;

-STISC employees do not use emails with the \*.ru extension for work purposes. If we receive

correspondence from \*.ru, then the answer is sent on paper with a handwritten signature to

legal address of the beneficiary in the Republic of Moldova. We do not reply electronically to an email

with \*.ru extension;

- STISC recommends all public system employees to avoid the use of mailboxes with the extension

\*.ru and migrate to the electronic mail system of public administration authorities, which in fact

and is massively used by public entities in accordance with normative provisions;

- Security of service information is another solid reason to use the government postal system,

given that the security of the system is ensured by applying technological and

principles of accessibility, integrity and confidentiality of information, and

in the event of a massive attack, the mechanism to protect government resources will be

exclusion of access to government resources from external sources."

Thus, the illegality of the use of @mail.ru or @rambler.ru emails in local and central public institutions, as well as the potential negative impact of this situation in terms of cybersecurity for the state system as a whole, was summarily illustrated. The use of mailboxes (created only by STISC with the ending \*.gov.md, \*apl.gov) by all state employees entailing a deeply strategic component in case of a general cyber-attack on the national digital infrastructure.

**The Ministry of Economic Development and Digitization of the Republic of Moldova (MDED), has come back with a legal clarification in this regard:**

"The regulatory framework governing the services of the electronic mail system within

public authorities are Government Decision No 822/2012 on the services of the electronic mail system

electronic mail system of public authorities and the Order of the Secretary General of the Government no. 67 of

07.06.2023 on the approval of the Regulation on the services of the electronic mail

electronic mail services of public administration authorities."

Well, if we go to analyze the documents, in point V. RESTRICTIONS AND LIMITATIONS of the Regulation of 2023 it is specified that "29. The user of electronic mail is prohibited from: 1) providing access to third parties to his own account for the use of the SPE". The very fact of using an @mail.ru mail domain in state institutions violates this restrictive point.

And in the above-mentioned government decision of 2012, even in paragraph 1 it is expressly stated: "On the creation of the Telecommunications System of Public Administration Authorities" (Official Gazette of the Republic of Moldova, 2004, No. 130, art. 1013), with subsequent amendments and additions, shall ensure the mandatory use by civil servants and other employees of public administration authorities of the services of the electronic mail system of public administration authorities for business correspondence and shall not allow the use of electronic mail services of third party providers for business correspondence." What could be legally clearer than not complying with these provisions, you might ask....

Government provisions and rulings have the force of law and are binding to be complied with. They are issued in accordance with the prerogatives and powers established by law and are intended to regulate various aspects of social, economic and political life in a country. Their status as normative acts subordinate to the law expresses that they are binding for compliance and implementation by public organizations and institutions.  
  
**We asked the current Minister of Energy, Victor Parlicov**, what he knows about the procedures and provisions in his ministry (with about 50 employees) regarding the use of e-mail services by civil servants. Here was the answer he received in the live broadcast of the Moldovan School of Journalism (on March 12, 2024): <https://youtu.be/fKIn4hHqDUw>

**Source:** Iurie Barbaroș, freelance journalist. Energy Minister Victor Parlicov's official video response. What the minister knows about his ministry's procedures and legal provisions regarding the use of electronic mail services by officials.

**The Public Services Agency of Moldova (ASP), through its Director Mircea Esanu,** comes with a valuable clarification (valid for all state organizations), namely:

"Within the Public Institution "Public Services Agency" (hereinafter ASP) there is no policy on

the use of concrete resources, including the ones listed by you (n.r. - @mail.ru, @rambler.ru, yandex.ru, bk.ru, pisem.net by the officials and employees of public institutions of the Republic of Moldova during their working hours). However, according to the ASP's internal regulations, employees are not allowed to

access on the Internet at automated workplaces sites containing information

entertaining, destructive, antisocial, etc., as well as information not directly related

with the performance of work duties, such as the use of personal mailboxes.

Thus, the ASP user/employee at the automated workplace uses

only governmental corporate electronic mail services and only for the purpose of

service:[https://www.legis.md/cautare/getResults?doc\_id=137723&lang=ro".](https://www.legis.md/cautare/getResults?doc_id=137723&lang=ro%22.%20)

But we get the best qualification of the situation from the Legal Directorate of the National Center for Personal Data Protection of the Republic of Moldova:

"pursuant to Art. 20 para. (1) lit. c) of Law no. 133/2011 on the protection

personal data, in the course of its activities, the CNPDCP has issued several

instructions on the processing of personal data in various areas, including,

electoral, police, educational, health, where it has emphasized to data controllers that,

disclosure by transmission of personal data over communication networks

that do not ensure an adequate level of protection of personal data (e.g:

sending information via personal e-mails such as @gmail.com,

@mail.ru, @yahoo.com, etc.) is to be prohibited.

At the same time, several information campaigns on the consequences of using systems/platforms foreign systems/platforms managed/created by non-resident operators, whose servers are located outside the country,

and the collection/processing of data through these systems/platforms may

result in loss of control over personal data and difficulty in

exercising, by the personal data subject, of the rights enshrined in

Personal Data Protection Act.

In this context, the NDCP has recommended data controllers, including,

public institutions which, in their day-to-day activity, process personal data

through communication networks or other digital storage and retention media, to ensure

encryption of this information or the use of a bilateral connection through secure channels

VPN.".

**The Legal Section of the National Center for Personal Data Protection (NCPDCP)** additionally came back with a supplement on the risks in personal data security, confidentiality of personal data and cross-border data transfer in cases when civil servants use personal e-mail addresses of the type @mail.ru, @rambler.ru, @yadex.ru, @bk.ru at work. It was specified that these e-mail platforms are frequently targeted by cyber-attacks, such as phishing or hacking, and personal personal data can be compromised. The full reply to our request is available here [here >>](https://fbi.md/datas/users/1-riscuri_centru_date_cp_acces_la_informaii_2.signed.pdf) 

**We asked the co-founder of the AO "Internet Community", Mr. Alexei Marciuc** for an expert comment on the associated security risks. The answer he received argues that "in general, it is not recommended to use mail on the .ru domain. Such [popular services in our country, such as Yandex and Mail.ru](https://www.nakanune.ru/articles/13994), are obliged to store user data, including all correspondence, audio and video content, for at least one year. All this information should be provided to relevant government agencies and law enforcement authorities upon official request. If we look at the open statistics, these services satisfy more than 70% of user data disclosure requests. In addition, they have been repeatedly featured in stories about user data leaks and the transfer of sensitive information to third parties. Official communications of public institutions and their officials need to be protected, especially when sensitive information and personal data are involved. Digital hygiene and basic cybersecurity rules are also a crucial issue that concerns all users and reduces risks." The full comment received can be [found here >>](https://fbi.md/datas/users/1-ao_comunitatea_internet.pdf)  
 [[](https://fbi.md/datas/users/1-ao_comunitatea_internet.pdf)](https://fbi.md/datas/users/1-ao_comunitatea_internet.pdf)

**Source**: Slide from Gladei & Partners presentation, by Iulian Pașatii. The area of secure and insecure zones for digital information. AIM Summit. 29.03.2024

So, with the legal issues and risks being clear, for us in election year 2024, the broader political, strategic and security context in which this use of \*.ru foreign domain emails in Moldova takes place becomes essential.

In Moldova's new Security Strategy, formulated in October 2023 by Maia Sandu, Russia is mentioned as a source of threat to Moldova's security. Being involved in systematic aggression against Ukraine and in hybrid operations against the Republic of Moldova, Russia is described as one of the most dangerous and persistent sources of threat to Moldova's statehood, democracy and prosperity (Moldova's Security Strategy: p.4, p.5, p.13, p.14 )

It is important to recall, in this context, that as of September 1, 2023, the online service platform Yandex provides its data (including from Central and South-Eastern Europe) about YandexGO customers to the Russian Federal Intelligence Service FSB without any limits, according to the [recent Meduza investigation](https://meduza.io/feature/2020/10/26/yandeks-vpervye-rasskazal-o-vydache-dannyh-rossiyan-po-zaprosam-vlastey).

Returning to the current political context in the Republic of Moldova which is of particular interest to us in a presidential election year... The latest pro-active SIS report of early February, 2024, on Russia's interference in the period 2024-2025, emphasizes that the Russian Federation aims to draw the Republic of Moldova into its sphere of influence. It is emphasized that Russia is using a hybrid mechanism for attacks against democratic processes and for undermining Moldova's European integration. Various means of intervention are described, such as financing pro-Russian political actors, using the mass media for manipulation and disinformation, involving foreign experts guided by the Administration of the Russian President, as well as creating crises in different areas to instigate social and ethnic tensions. It also highlights the strategies planned for the period 2024-2025, which include compromising the referendum on European integration, meddling in the presidential elections and creating a pro-Russian or at least moderate majority in the Moldovan Parliament (p.2, p.7, p.4 in the report).  
  
On 18 March 2024, at the Palatul Republic, Maia Sandu was elected as the President of the Republic of Moldova for the first time, after having used the statutory function of the email address @mail.ru for the new no-strategy for securitisation formulated in October 2023. Iată răspunsul pe care l-am primit: <https://youtu.be/lPzRM0XG36I>.

**Sursa**: Iurie Barbaroș, independent journalist. Official video reply of the President of the Republic of Moldova, Maia Sandu. How the president is commenting the use of @mail.ru services in public institutions.

Objectively, the policy on confidentiality from @Mail.ru reveal in line [3.4 (Processing and Transmission of Information)](http://help.mail.ru/legal/terms/common/privacy?signupid=lu9oib62i6c)) such riscs as as disclosing private information to third parties. ‘The Company may transfer Users' Account and Other Data to third parties, subject to the purposes and grounds set out in this Policy. Such third parties may include: - any public authority or local government body to which the Company is obliged to provide information in accordance with applicable law upon request.’

At a press conference on March 18, 2024, at the Palace of the Republic, Maia Sandu was asked how the use of @mail.ru by state officials fits in with our new security strategy formulated in October, 2023. Here is the answer we received: <https://youtu.be/lPzRM0XG36I>  
**Owners and stakeholders of @Mail.ru Group and @Rambler.ru Group**

We tried to find out from open and verified sources who the ultimate owners of @Mail.ru Grup are.

The media project "Север.Реалиии" of the Russian service [Radio Libera (a subsidiary of Free Europe) wrote that in October 2021](https://www.severreal.org/a/kompaniya-usm-alishera-usmanova-prodala-vk-sogazu/31590547.html) Mail.ru Holding had already announced in October 2021 that it would change its name to VK. The company described the rebranding as a continuation of the development of its ecosystem, with the VKontakte social network at its center.

In late November, Sberbank also sold its stake in VK to Gazprombank. Thus, the structures, one way or another linked to Gazprom, consolidate the absolute majority of voting shares in VK, Kommersant notes (the publication is also owned by Usmanov's structures).

On December 2, 2021, it was announced that the USM Holding Company of businessman [Alisher Usmanov (a major financier of the war in Ukraine)](https://war-proekt.media/spisok-oligarkhov/provider/alisher-usmanov/) sold its voting stake in VK (formerly Mail.ru) to Sogaz Group.

The global media company [Forbes writes about](https://www.forbes.ru/milliardery/382745-zagadka-sogaza-kogo-krome-milliardera-kovalchuka-i-dvoyurodnogo-plemyannika-putina-obogatil-strahovshchik-gazproma) the ultimate owners of Sogaz Group in the article "The Sogaz mystery: who, apart from billionaire Kovalchuk and Putin's great-grandson, got rich from the insurer Gazprom?"

"Shortly before the merger of the insurance assets of VTB and Sogaz, an unknown person bought a 12.5% stake in Gazprom's insurance company for about 23 billion rubles. Subsequently, the majority of this stake was acquired by Sogaz for 55 billion rubles. The emergence of Russia's largest insurance company has also enriched billionaire Yuri Kovalchuk (a major sponsor of the war in Ukraine, according to [War Proekt](https://war-proekt.media/spisok-oligarkhov/provider/yuriy-kovalchuk/)), a great-grandson of President Mikhail Shelomov and former adviser to Igor Secin, by hundreds of millions of dollars."  
  
**Therefore, the real owners of the @Mail.Ru (Group) service, more recently VK Group, the most popular in Moldova (according to the** [**TNS Gallup report**](https://ru.wikipedia.org/wiki/%D0%9F%D0%BE%D1%87%D1%82%D0%B0_Mail.ru)**) are people in Putin's immediate entourage. Both** [**Secin**](https://ekaterinburg.bezformata.com/listnews/sechin-dejstvuyushij-general-fsb/57086087/) **I., as well as Putin and Vladimir Kirienko (CEO of VK Grup from 2021, son of Kremlin official Sergey Kiriyenko) being associated with Russian special services FSB (ex-КGB). Most of them also** [**being on the American and European OFAC and SDN**](https://ofac.treasury.gov/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists) **sanctions list.**

**The web portal Rambler.ru**, one of the largest in Russia, is owned by Rambler Media Group. The website, launched in 1996 by Stack Ltd, went public in 2005, was acquired by Prof-Media in 2006, and was later [acquired by the Russian bank Sberbank](https://www.bbc.com/russian/news-54740908) (in 2019).

The majority shareholder of Sberbank is the Russian National Property Fund, managed by the Government of Russia (until 2020 the Central Bank of the Russian Federation), which owns 50%+1 of Sberbank's voting shares. The remaining shares are dispersed among portfolio, private and other investors.

Sberbank has been on the [US Treasury Department's sanctions list since February 24](https://home.treasury.gov/news/press-releases/jy0608), 2022 and under sanctions from the [UK government since March 1, 2022](https://assets.publishing.service.gov.uk/media/64a6947d7a4c23000cbba27a/Notice_Russia_060723.pdf). The bank has been sanctioned by the UK government on the grounds that it has been involved in obtaining a benefit from, or assisting the government of Russia by conducting business as an entity affiliated with the government of Russia and in a strategically important sector (financial services).  
  
  
***To summarize it all, some public officials in Moldova continue to use for business purposes e-mail platforms whose final beneficiaries include persons affiliated with Putin and Russian special services, as well as Russian central banking entities, sanctioned both in the US and in Europe for manipulation of the financial services market and for financing the criminal war in Ukraine.***  
  
**Who has discussed the issue of using @Mail.ru in Moldova so far?**

Historically, several state and non-state actors have warned about the danger of the use of foreign Russian email platforms by state officials. In [2012, the round table](http://old.egov.md/en/communication/news/make-yourself-home-cyberspace-be-safe) "Aspects of interaction between providers of electronic communication networks and services and state bodies on the implementation of the security policy of the infrastructure security of the users of the services and transmitted data" was organized.

According to the then participants, many public officials use the services mail.ru, rambler.ru or gmail.com instead of professional .md Internet domain addresses, which is neither correct nor secure. They reiterated the need to implement the interoperability framework, a platform that would facilitate the secure exchange of data between public authorities.

In 2019, [Agora wrote the article](https://agora.md/stiri/56100/Tara-mail-ru--adresele-de-e-mail-ale-primariilor-din-r--moldova--create-arbitrar-de-functionarii-locali) "Country mail.ru. E-mail addresses of Moldovan city halls arbitrarily created by local officials" in which it talked about the use of personal e-mail addresses for official correspondence and the fact that the law exists but is not enforced in Moldova.

In 2022, Parliament Speaker [Igor Grosu appeared in a video](https://newsmaker.md/ro/video-grosu-le-cere-functionarilor-de-stat-sa-renunte-la-mail-ru/) on NewsMaker in which he urged employees of state institutions not to use email with the ".ru" extension in order to protect themselves against possible cyber threats (a topic he also discussed in the Commission on Exceptional Situations in Moldova).

In this specific context, the use of Russian e-mail services (be it @mail.ru, @rambler.ru or yandex.ru, bk.ru, pisem.net, etc.) **in the daily work of Moldovan civil servants is clearly detrimental to the national security of the state** and is de facto and de jure illegal.

Author: Iurie Barbaroș Jr, Independent Journalist  
23|03|2024    18:40