Media Diversity Institute

DIGITAL RIGHTS AND CORPORATE ACCOUNTABILITY IN ARMENIA

Samvel Martirosyan

Yerevan
2023

DIGITAL RIGHTS AND CORPORATE ACCOUNTABILITY IN ARMENIA

Samvel Martirosyan

CONTENT

Preface

The issue of Digital Rights is not a widely discussed topic in Armenia because Armenians are unaware of these rights and quite possibly their impact on their political and democratic well-being.

Armenia is ranked as a free country in the Freedom on the Net report by Freedom House. But there are a lot of issues related to digital rights, privacy, and potential threats that are hidden.

According to the Public Services Regulatory Commission (PSRC) of the Republic of Armenia[i] the fixed broadband penetration rate is about 17%, while mobile broadband internet penetration is about 96% (Data of 2021). Almost 100% of the territory of Armenia is covered by the mobile network (excluding some unpopulated mountainous parts of the country). This means that the mobile internet has a vital role in communications in the country, and that the telecom operators have a huge role on safeguarding their users' privacy.

This research uses Ranking Digital Rights (RDR) Index Methodology to assess how Armenia's three telecom operators (Viva-MTS, Team Telecom, and Ucom) collect, store, process, and share users' data with third parties and government agencies.

The research finds that all three companies provide similar documents to inform their customers, yet they do not provide enough details about how they use and share users' data with third parties or government agencies.

While all companies refer to Armenian legislation in their public terms and conditions, privacy policies and related texts, they do not specify what laws or regulations apply to their services or customers' rights.

Additionally, while the research finds and highlights differences between the three companies regarding the collection of users' data, overall, the information provided is limited, and the companies do not outline the limits of their data collection.

History of internet blockings

Officially in Armenia internet resources are not blocked. There is no legislation allowing any type of content blocking. There are some possibilities during the state emergency or martial law, but not in peaceful regular times.

On the other hand, there are some cases when the government used its power to block some internet resources. There were no official statements during all blockages.

The first time when the internet was censored in Armenia was in the aftermath of March 1, 2008 events when following the presidential elections, clashes between oppositional and police and army forces led to the death of 10 people. President Robert Kocharyan, with the approval of the Armenian parliament, declared a 20-day state of emergency, banning future demonstrations and censoring the media from broadcasting any political news except those issued by official state press releases.[ii]

On March 2, 2008, at around 11:00 pm, Internet providers (according to non-official sources, the order was given by the National Security Service[iii]) began blocking the entrance of Armenian users to several Armenian media and opposition organization websites. For several days YouTube was blocked as well. Blockage continues until the end of the state of emergency, March 21, 2008.[iv]

After 2008 for years in Armenia, no sites were blocked. The next case happened in 2016. On July 17, during the initial assault on the police station, internet users reported that they were unable to access Facebook through major ISPs, including Armentel (Team Telecom now) and Ucom. News reports said connectivity was restored within approximately 40 minutes. Facebook confirmed that “a disruption affecting access to Facebook products and services” had taken place in Armenia, coinciding with protests. This Facebook blocking also was one of the reasons why Armenia was declared as a country with partly free internet in the Freedom on the Net report (before and after the country was declared with free internet).[v]

The next blocking was done during the Karabakh war in the fall of 2020. The war started on September 27. Four days later, on October 1, 2020, users faced problems with the TikTok social network. State news agency Armenpress reported that TikTok was inaccessible to some users, while others had trouble downloading videos or watching videos they had already downloaded, while there is no official information about blocking.[vi] The government did not confirm involvement, but issues loading the platform and uploading content persisted for several weeks.

From the second half of October 2020 until the ceasefire agreement on November 10, many Turkish and Azerbaijani media outlets, and governmental resources with .az and .tr domains were inaccessible. Issues with accessing the sites continued for months after the ceasefire. There was no official recognition of the blockage by ISPs or the Armenian government.[vii]

The next time ISP starts the blocking with the same scenario. In 2022 September Azerbaijan attacks Armenia, and heavy military clashes started along the border.[viii] Hours later TikTok again was blocked in Armenia, and its accessibility was restored 10 days after.[ix]

However, neither the government nor service providers confirmed whether there was an official order to block the platform.

Data Leaks

Armenia remains a country with a high risk of personal data leaks. One of the main reasons is a permanent conflict between Armenia and Azerbaijan around Artsakh (Nagorno-Karabakh Republic). This conflict is also marked by the involvement of many patriotic and state-sponsored hacking groups from Azerbaijan (and sometimes from Turkey) attacking websites, social network users and infrastructure.

As a result, big sets of personal data are stolen by hackers and very often openly leaked on the Internet. For example, in 2020 there were minimum 2 cases where leaked data was related to the mobile operators[x]:

- On July 17, a third-party SMS text message operator was compromised and about 3,000 Armenian mobile subscribers received SMS messages, which appeared to be sent from the Armenian Ministry of Defense.

- On November 9, Azerbaijani hackers published a phone database of Karabakh Telecom (mobile operator of Nagorno-Karabakh Republic) customers, featuring more than 58,000 records, including the addresses and phone numbers of Artsakh President Arayik Harutyunyan, his administration, MPs, and military officials. The database also includes data of citizens of the Republic of Armenia, widely using Karabakh Telecom services.

Data processing and usage of algorithms

While the Ranking Digital Rights Index indicators are not based on Armenia's legal code, nor do they view the compliance of the Armenian telecoms to their legal obligations, it is useful to have an overview of the legal framework, under which those companies operate.

In general, personal data operation, and processing in Armenia are regulated by Personal Data Protection Law, adopted in 2015[xi]. The Law requires that personal data processing must have a legitimate purpose and use the minimum amount of data needed. It also forbids processing data that are irrelevant or can be anonymized. Personal data must not be stored longer than necessary for the abovementioned legitimate purpose.

There are no specific regulations related to the usage of algorithms and related technical-specific methods. There is no public discourse or other narratives related to the issue.

During the COVID-19 quarantine period in 2020, the Armenian government declared a state of emergency, which was followed by the National Assembly's authorization for the government to track individuals using data obtained from mobile operators. In order to process the meta-data of all mobile phone calls, SMS messages, and geo-location data from mobile operators, the government implemented special software that utilized machine learning and big data analysis[xii].The system created by a company that remained unknown (the government did not want to disclose information about the creator of the software) aggregated and analyzed all metadata and geolocation data from all three mobile operators[xiii]. The collected data was utilized to determine the extent of exposure of infected individuals and was subsequently stored on the server of the e-Governance Infrastructure Implementation Agency (EKENG). The National Security Service (NSS) was responsible for overseeing the software's execution and ensuring its security.

During a National Assembly meeting on April 13, Tigran Avinyan, the head of the Crisis Management Center and also the Deputy Prime Minister, explained that following the amendment to the Law on the Legal Regime of the State of Emergency, which allowed for the monitoring of phone calls and imposed restrictions on the protection of personal data, privacy, and freedom of communication, the system analyzed the data of 3,029 individuals. The analysis led to the self-isolation of 7,000 individuals. Bagrat Badalyan, an advisor to Deputy Prime Minister Avinyan, stated that the content and duration of the calls were not of interest, nor were they collected.

The system worked until the end of September 2020. On 25 September 2020, all collected metadata was destroyed in a presence of representatives of the government, the National Assembly, and three mobile operators. All hardware devices on which the information was stored were also physically destroyed.[xiv]

There was no public control over the data used by the government.

Mobile operators of Armenia

There are 3 mobile operators in Armenia: Viva-MTS, Team Telecom, and Ucom.

Viva-MTS ("MTS Armenia" CJSC) ("VivaCell" at founding), the company with the biggest mobile-users share in the Armenian market, obtained a license for the implementation of activities in 2004 and launched in 2005. In September 2007, after the sale of 80% of the shares, the company became a subsidiary of the Russian company "Mobile TeleSystems" ("MTS"). As a result of the co-branding carried out in 2008, the Company's brand changed. VivaCell became VivaCell-MTS. In April 2009, Viva-MTS announced the commercial launch of its third-generation (3G) network. For the first time in Armenia, a 3G network was launched in the regions. Viva-MTS launched 4G/LTE network for the first time in Armenia in 2010. In August 2019, MTS acquired the remaining 20% of Viva-MTS shares. Viva-MTS has its own fiber-optical cable network throughout the country, extending from the north of Armenia to the south.The Company imports Internet through its channels for the needs of the domestic market. The company currently has about 1,200 employees and over 2 million subscribers. According to recent information, Viva-MTS, possibly, is up for sale[xv].

Telecom Armenia CJSC was founded as "Armentel" in March 1995 as a successor of the whole Soviet time telecom system of Armenia. On November 3, 2006, it became a subsidiary of the Russian corporation VimpelCom (later called VEON) and started operating under the Beeline brand. The company was renamed to “VEON Armenia” in 2017. On October 29, 2020, TEAM LLC acquired 100% of the company's shares using credit funds, and renamed the company to "Telecom Armenia CJSC". Telecom Armenia currently belongs to "TEAM LLC", which was founded by Hayk and Alexandr Yesayan, the former top managers of another telecom company Ucom. Since May 2022, the company operates under the brand Team Telecom.

Ucom was founded in 2009 as an internet services provider, including IPTV. In 2013, the company received a license to provide public mobile internet services, and in 2015 acquired a 100% stake in Orange Armenia (the Armenian branch of telecommunications company Orange S.A.), thus entering the Armenian mobile market.

Market share of the Mobile Operators

As of the third quarter data of 2022, there are 3,921,230 mobile subscribers in Armenia. Viva-MTS remains the leading operator by the number of subscribers. As of the third quarter data of 2022, the number of subscribers of the operator was 2,306,396. Team Telecom (formerly Beeline) is in second place. As of the third quarter data of 2022, the number of subscribers of the company was 960,923. In third place is Ucom. As of the third quarter data of 2022, the number of subscribers of the company was 653,911[xvi].

Methodology and Findings

Methodology

Using the 2020 Ranking Digital Rights (RDR) Index Methodology[xvii], this Report evaluates the Human Rights practices of all 3 Armenian mobile operators: Viva-MTS, Team Telecom Armenia, and Ucom. We reviewed the situation related to the pre-paid mobile services. It can be stated that the situation with all other services offered by the mobile operators is largely the same, companies, in general, are not distinguishing regulations between different mobile services.

Ranking Digital Rights (RDR) is a non-profit organization that works to promote freedom of expression and privacy on the internet. RDR has developed a comprehensive set of standards used to evaluate a company's commitment to human rights and policy disclosures. The RDR standard comprises 58 indicators across three categories: governance, freedom of expression as well as information and privacy.

Twenty-two indicators in two groups are used in the study, namely:

F: Freedom of Expression and Information

F1a: Access to terms of service
F2a: Changes to terms of service
F3a: Process for terms of service enforcement
F4a: Data about content restrictions to enforce terms of service
F4b: Data about account restrictions to enforce terms of service
F5a: Process for responding to government demands to restrict content or accounts
F5b: Process for responding to private requests for content or account restriction
F6. Data about government demands to restrict content and accounts
F7. Data about private requests for content or account restriction
F8. User notification about content and account restriction
F9. Network management (telecommunications companies)
F10. Network shutdown (telecommunications companies)

P: Privacy

P1(a). Access to privacy policies
P3(a). Collection of user information
P4. Sharing of user information
P5. Purpose for collecting, inferring, and sharing user information
P6. Retention of user information
P7. Users' control over their own user information
P8. Users' access to their own user information
P10a. Process for responding to government demands for user information
P10b. Process for responding to private requests for user information
P15. Data breaches

Indicators

The freedom of expression and information indicators are identified with the letter "F". "Indicators in this category seek evidence that the company demonstrates that it respects the right to freedom of expression and information, as articulated in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights and other international human rights instruments. The company's disclosed policies and practices must demonstrate how it avoids actions that may interfere with this right, except where such actions are lawful, proportionate, and for a justifiable purpose. Companies that perform well on this indicator demonstrate a strong public commitment to transparency not only in terms of how they respond to government and others' demands, but also in how they determine, communicate, and enforce private rules and commercial practices that affect users' fundamental rights to freedom of expression and information." (Ranking Digital Rights, n.d.).

Below are the "F" indicators used in this Report:[xviii]

F1(a). Access to terms of service

The company should offer terms of service that are easy to find and easy to understand.

Elements:

1. Are the company's terms of service easy to find?
2. Are the terms of service available in the primary language(s) spoken by users in the company's home jurisdiction?
3. Are the terms of service presented in an understandable manner?

F2(a). Changes to terms of service

The company should clearly disclose that it directly notifies users when it changes its terms of service, prior to these changes coming into effect.

Elements:

1. Does the company clearly disclose that it directly notifies users about all changes to its terms of service?
2. Does the company clearly disclose how it will directly notify users of changes?
3. Does the company clearly disclose the timeframe within which it directly notifies users of changes prior to these changes coming into effect?
4. Does the company maintain a public archive or change log?

F3(a). Process for terms of service enforcement

The company should clearly disclose the circumstances under which it may restrict content or user accounts.

Elements:

1. Does the company clearly disclose what types of content or activities it does not permit?
2. Does the company clearly disclose why it may restrict a user's account?
3. Does the company clearly disclose information about the processes it uses to identify content or accounts that violate the company's rules?
4. Does the company clearly disclose how it uses algorithmic systems to flag content that might violate the company's rules?
5. Does the company clearly disclose whether any government authorities receive priority consideration when flagging content to be restricted for violating the company's rules?
6. Does the company clearly disclose whether any private entities receive priority consideration when flagging content to be restricted for violating the company's rules?
7. Does the company clearly disclose its process for enforcing its rules once violations are detected?

F4(a). Data about content restrictions to enforce terms of service

The company should clearly disclose and regularly publish data about the volume and nature of actions taken to restrict content that violates the company's rules.

Elements:

1. Does the company publish data about the total number of pieces of content restricted for violating the company's rules?
2. Does the company publish data on the number of pieces of content restricted based on which rule was violated?
3. Does the company publish data on the number of pieces of content it restricted based on the format of content? (e.g. text, image, video, live video)?
4. Does the company publish data on the number of pieces of content it restricted based on the method used to identify the violation?
5. Does the company publish this data at least four times a year?
6. Can the data be exported as a structured data file?

F4(b). Data about account restrictions to enforce terms of service

The company should clearly disclose and regularly publish data about the volume and nature of actions taken to restrict accounts that violate the company's rules.

Elements:

1. Does the company publish data on the total number of accounts restricted for violating the company's own rules?
2. Does the company publish data on the number of accounts restricted based on which rule was violated?
3. Does the company publish data on the number of accounts restricted based on the method used to identify the violation?
4. Does the company publish this data at least four times a year?
5. Can the data be exported as a structured data file?

F5(a). Process for responding to government demands to restrict content or accounts

The company should clearly disclose its process for responding to government demands (including judicial orders) to remove, filter, or restrict content or accounts.

Elements:

1. Does the company clearly disclose its process for responding to non-judicial government demands?
2. Does the company clearly disclose its process for responding to court orders?
3. Does the company clearly disclose its process for responding to government demands from foreign jurisdictions?
4. Do the company's explanations clearly disclose the legal basis under which it may comply with government demands?
5. Does the company clearly disclose that it carries out due diligence on government demands before deciding how to respond?
6. Does the company commit to pushing back on inappropriate or overbroad demands made by governments?
7. Does the company provide clear guidance or examples of implementation of its process of responding to government demands?

F5(b). Process for responding to private requests for content or account restriction

The company should clearly disclose its process for responding to requests to remove, filter, or restrict content or accounts that come through private processes.

Elements:

1. Does the company clearly disclose its process for responding to requests to remove, filter, or restrict content or accounts made through private processes?
2. Do the company's explanations clearly disclose the basis under which it may comply with requests made through private processes?
3. Does the company clearly disclose that it carries out due diligence on requests made through private processes before deciding how to respond?
4. Does the company commit to pushing back on inappropriate or overbroad requests made through private processes?
5. Does the company provide clear guidance or examples of implementation of its process of responding to requests made through private processes?

F6. Data about government demands to restrict content and accounts

The company should regularly publish data about government demands (including judicial orders) to remove, filter, or restrict content and accounts.

Elements:

1. Does the company break out the number of government demands it receives by country?
2. Does the company list the number of accounts affected?
3. Does the company list the number of pieces of content or URLs affected?
4. Does the company list the types of subject matter associated with the government demands it receives?
5. Does the company list the number of government demands that come from different legal authorities?
6. Does the company list the number of government demands it knowingly receives from government officials to restrict content or accounts through unofficial processes?
7. Does the company list the number of government demands with which it complied?
8. Does the company publish the original government demands or disclose that it provides copies to a public third-party archive?
9. Does the company report this data at least once a year?

F7. Data about private requests for content or account restriction

The company should regularly publish data about requests to remove, filter, or restrict access to content or accounts that come through private processes.

Elements:

1. Does the company break out the number of requests to restrict content or accounts that it receives through private processes?
2. Does the company list the number of accounts affected?
3. Does the company list the number of pieces of content or URLs affected?
4. Does the company list the reasons for removal associated with the requests it receives?
5. Does the company clearly disclose the private processes that made requests?
6. Does the company list the number of requests it complied with?
7. Does the company publish the original requests or disclose that it provides copies to a public third-party archive?
8. Does the company report this data at least once a year?
9. Can the data be exported as a structured data file?
10. Does the company clearly disclose that its reporting covers all types of requests that it receives through private processes?

F8. User notification about content and account restriction

The company should clearly disclose that it notifies users when it restricts content or accounts.

Elements:

1. N/A
2. Does the company clearly disclose that it notifies users who attempt to access content that has been restricted?

3. In its notification, does the company clearly disclose a reason for the content restriction (legal or otherwise)?
4. Does the company clearly disclose that it notifies users when it restricts their accounts?

F9. Network management (telecommunications companies)

The company should clearly disclose that it does not prioritize, block, or delay certain types of traffic, applications, protocols, or content for any reason beyond assuring the quality of service and reliability of the network.

Elements:

1. Does the company clearly disclose a policy commitment to not prioritize, block, or delay certain types of traffic, applications, protocols, or content for reasons beyond assuring the quality of service and reliability of the network?
2. Does the company engage in practices, such as offering zero-rating programs that prioritize network traffic for reasons beyond assuring the quality of service and reliability of the network?
3. If the company does engage in network prioritization practices for reasons beyond assuring the quality of service and reliability of the network, does it clearly disclose its purpose for doing so?

F10. Network shutdown (telecommunications companies)

The company should clearly disclose the circumstances under which it may shut down or restrict access to the network or to specific protocols, services, or applications on the network.

Elements:

1. Does the company clearly disclose the reason(s) why it may shut down service to a particular area or group of users?
2. Does the company clearly disclose why it may restrict access to specific applications or protocols (e.g., VoIP, messaging) in a particular area or to a specific group of users?
3. Does the company clearly disclose its process for responding to government demands to shut down a network or restrict access to a service?
4. Does the company clearly disclose a commitment to push back on government demands to shut down a network or restrict access to a service?
5. Does the company clearly disclose that it notifies users directly when it shuts down a network or restricts access to a service?
6. Does the company clearly disclose the number of network shutdown demands it receives?
7. Does the company clearly disclose the specific legal authority that makes the demands?
8. Does the company clearly disclose the number of government demands with which it complied?

Privacy indicators start with the letter “P”. “Indicators in this category seek evidence that in its disclosed policies and practices, the company demonstrates concrete ways in which it respects the right to user privacy as articulated in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights and other international human rights instruments. The policies should also demonstrate a strong commitment to protecting users' digital security. Companies that perform well on these indicators demonstrate a strong public commitment to transparency not only in terms of how they respond to government and others' demands, but also in how they determine, communicate, and enforce private rules and commercial practices that affect users' privacy.” (Ranking Digital Rights, n.d.).

Below are the Privacy indicators used in this Report:

P1(a). Access to privacy policies

The company should offer privacy policies that are easy to find and easy to understand.

Elements:

1. Are the company’s privacy policies easy to find?
2. Are the privacy policies available in the primary language(s) spoken by users in the company’s home jurisdiction?
3. Are the policies presented in an understandable manner?
4. (For mobile ecosystems): Does the company disclose that it requires apps made available through its app store to provide users with a privacy policy?
5. (For personal digital assistant ecosystems): Does the company disclose that it requires skills made available through its skill store to provide users with a privacy policy?

P3(a). Collection of user information

The company should clearly disclose what user information it collects and how.

Elements:

1. Does the company clearly disclose what types of user information it collects?
2. For each type of user information the company collects, does the company clearly disclose how it collects that user information?
3. Does the company clearly disclose that it limits the collection of user information to what is directly relevant and necessary to accomplish the purpose of its service?

P4. Sharing of user information

The company should clearly disclose what user information it shares and with whom.

Elements:

1. For each type of user information the company collects, does the company clearly disclose whether it shares that user information?
2. For each type of user information the company shares, does the company clearly disclose the types of third parties with which it shares that user information?
3. Does the company clearly disclose that it may share user information with government(s) or legal authorities?
4. For each type of user information the company shares, does the company clearly disclose the names of all third parties with which it shares user information?

P5. Purpose for collecting, inferring, and sharing user information

The company should clearly disclose why it collects, infers, and shares user information.

Elements:

1. For each type of user information the company collects, does the company clearly disclose its purpose for collection?
2. For each type of user information the company infers, does the company clearly disclose its purpose for the inference?
3. Does the company clearly disclose whether it combines user information from various company services and if so, why?
4. For each type of user information the company shares, does the company clearly disclose its purpose for sharing?
5. Does the company clearly disclose that it limits its use of user information to the purpose for which it was collected or inferred?

P6. Retention of user information

The company should clearly disclose how long it retains user information.

Elements:

1. For each type of user information the company collects, does the company clearly disclose how long it retains that user information?
2. Does the company clearly disclose what de-identified user information it retains?
3. Does the company clearly disclose the process for de-identifying user information?
4. Does the company clearly disclose that it deletes all user information after users terminate their accounts?
5. Does the company clearly disclose the time frame in which it will delete user information after users terminate their accounts?

P7. Users' control over their own user information

The company should clearly disclose to users what options they have to control the company's collection, inference, retention, and use of their user information.

Elements:

1. For each type of user information the company collects, does the company clearly disclose whether users can control the company's collection of this user information?
2. For each type of user information the company collects, does the company clearly disclose whether users can delete this user information?
3. For each type of user information the company infers on the basis of collected information, does the company clearly disclose whether users can control if the company can attempt to infer this user information?
4. For each type of user information the company infers on the basis of collected information, does the company clearly disclose whether users can delete this user information?
5. Does the company clearly disclose that it provides users with options to control how their user information is used for targeted advertising?
6. Does the company clearly disclose that targeted advertising is off by default?
7. Does the company clearly disclose that it provides users with options to control how their user information is used for the development of algorithmic systems?
8. Does the company clearly disclose whether it uses user information to develop algorithmic systems by default, or not?

P8. Users' access to their own user information

Companies should allow users to obtain all of the user information the company holds.

Elements:

1. Does the company clearly disclose that users can obtain a copy of their user information?
2. Does the company clearly disclose what user information users can obtain?
3. Does the company clearly disclose that users can obtain their user information in a structured data format?
4. Does the company clearly disclose that users can obtain all public-facing and private user information a company holds about them?
5. Does the company clearly disclose that users can access the list of advertising audience categories to which the company has assigned them?
6. Does the company clearly disclose that users can obtain all the information that a company has inferred about them?

P10(a). Process for responding to government demands for user information

The company should clearly disclose its process for responding
to the government's demands for user information.

Elements:

1. Does the company clearly disclose its process for responding to non-judicial government demands?
2. Does the company clearly disclose its process for responding to court orders?

3. Does the company clearly disclose its process for responding to government demands from foreign jurisdictions?
4. Do the company's explanations clearly disclose the legal basis under which it may comply with government demands?
5. Does the company clearly disclose that it carries out due diligence on government demands before deciding how to respond?
6. Does the company commit to pushing back on inappropriate or overbroad government demands?
7. Does the company provide clear guidance or examples of implementation of its process for government demands?

P10(b). Process for responding to private requests for user information

The company should clearly disclose its process for responding to requests for user information that come through private processes.

Elements:

1. Does the company clearly disclose its process for responding to requests made through private processes?
2. Do the company's explanations clearly disclose the basis under which it may comply with requests made through private processes?
3. Does the company clearly disclose that it carries out due diligence on requests made through private processes before deciding how to respond?
4. Does the company commit to pushing back on inappropriate or overbroad requests made through private processes?
5. Does the company provide clear guidance or examples of implementation of its process of responding to requests made through private processes?

P15. Data breaches

The company should publicly disclose information about its processes for responding to data breaches.

Elements:

1. Does the company clearly disclose that it will notify the relevant authorities without undue delay when a data breach occurs?
2. Does the company clearly disclose its process for notifying data subjects who might be affected by a data breach?
3. Does the company clearly disclose what kinds of steps it will take to address the impact of a data breach on its users?

Evaluation and scoring

Companies receive a cumulative score across all RDR Index categories. The results show how companies performed by each category and indicator. The RDR Index evaluates institutional disclosure of the overarching "parent" or "group", as well as those of selected services and/or local operating companies, depending on company structure. Each indicator has a list of elements, and companies receive credit (full, partial or no credit) for each element they fulfill. The evaluation covers disclosure for every element of each indicator, based on one of the following possible answers:

- "Yes"/ full disclosure: Company disclosure meets the element requirement.
- "Partial": Company disclosure has met some but not all aspects of the element, or the disclosure is not comprehensive enough to satisfy the full scope of the element.
- "No disclosure found": Researchers were unable to find the information provided by the company on its website that answers the element question.
- "No": Company disclosure exists, but it specifically does not disclose to users what the element is asking. This is distinct from the option of "no disclosure found," although both result in no credit.
- "N/A": Not applicable. This element does not apply to the company or service. Elements marked as N/A will not be counted for or against a company's score

Points

- Yes/full disclosure = 100
- Partial = 50
- No = 0
- No disclosure found = 0
- N/A = excluded from score and averages

Findings

Multiple significant findings have been identified.

To begin with, all three mobile operators in Armenia appear to inform their customers in a similar manner. There is a lack of substantial variance in their general terms and data protection strategies. This implies that telecommunication and other comparable businesses in the region may have a common approach.

Furthermore, information on how user data is used by operators, third-party companies, and government agencies is limited. Operators generally disclose that they use personal data for technical and legal purposes and share some data with third-parties, but fail to provide specific details of such sharing and data use.

Operators tend to avoid providing detailed information and instead highlight the Armenian legislation without any explicit references or specifics.

Finally, with regards to data protection issues, operators do not differentiate between pre-paid and post-paid mobile services.

Freedom of Expression and Information

There are no published transparency reports by the companies about government demands (including judicial orders) to remove, filter, or restrict content or accounts. There is no information about processes of response to the government or private demands to requests to remove, filter, or restrict content or accounts.

All 3 companies have placed all information regarding users' rights and other related details in 2 big documents - general terms and data protection policy.

In the case of Viva-MTS these are:

- General Terms of Provisioning Mobile Electronic Communication Services[xix]
- Privacy Policy[xx]

Team Telecom Armenia:

- General Terms And Conditions For The Provision Of Electronic Communication And Other Services[xxi]
- Privacy Policy[xxii]

Ucom:

- General Terms And Conditions For Provision Of Electronic Communication And Other Related Services[xxiii]
- Personal Data Processing Policy/ Notice On Personal Data Processing[xxiv]

All documents are presented on the web-sites of the companies, in visible places, the customer needs 1-2 clicks to get the information. All files are presented in 3 languages: Armenian, English, and Russian. This meets the customers' language needs, and the documents are understandable for the customers.

All operators are properly informing users about changes in terms of service, which is included in General Terms documents. In Viva-MTS it is 3 days prior to publishing: "The Operator is entitled to make a public offer at his discretion on the amendment of Contract terms, including the applied tariff plans, tariffs, and regulations, by publishing the present amendments not less than 3 (three) days prior to publishing on the Operator's official website and/or announcing in the service centers, as well as placing a public announcement, if necessary, at least in one mass media, widely spread throughout the Republic of Armenia".[xxv] In Team Telecom it is 10 days: "The Operator shall be entitled from time to time to make changes and additions (unilaterally) in the Subscription Agreement, including these Terms and Conditions, which shall be published on the Operator's website 10 (ten) days before the entry into force for mobile services (which are also available via a call to the Call Center or a visit to the Sales and Service Centers)."[xxvi] In Ucom it is 7 days: "Ucom is entitled to at any time make (unilaterally) amendments and supplements to the Subscription Agreement, including to these Terms, which shall be published on Ucom website (which may be made available to You by contacting Call Center or visiting Sales and Service Centers) seven (7) days prior to the entry into force thereof, except for the change to the scope of television channels included in the Service(s) and/or change to the content of television programs of television channels broadcasting (rebroadcasting) by Ucom or termination thereof, which shall enter into force after three (3) days following the publication on the Website."[xxvii]

But all 3 companies are not maintaining any public archive or change log of Terms of Services.

There is no concrete information about the content or user restriction. Companies are not publishing any data related to the quality and quantity of restricted content, or blocked users.

All information related to the indicators F3(a), F4(a), F4(b), F5(a), F5(b), F6, F7, F8, F10 for all 3 mobile operators is not disclosed.

Information about indicator F9 is also mostly not disclosed. Companies are not speaking about network neutrality, or not prioritizing, blocking, or delaying certain types of traffic, applications, protocols, or content for any reason beyond assuring the quality of service and reliability of the network. But in reality, all 3 companies have several mobile tariffs with unlimited internet data for top apps - social media, streaming services, and messengers[xxviii].

Privacy

All 3 companies have placed the information about personal data in one document on data protection policy.

In the case of Viva-MTS it is:
- Privacy Policy[xxix]

Team Telecom Armenia:
- Privacy Policy[xxx]

Ucom:
- Personal Data Processing Policy/ Notice On Personal Data Processing[xxxi]

All documents are presented on the web-sites of the companies, in visible places, the customer needs 1-2 clicks to get the information. All files are presented in 3 languages: Armenian, English, and Russian. This meets the customers' language.

In the case of the collection of users' data (indicator P3(a) there is some difference between companies. Viva-MTS possible to find information about data collected from subscribers: In terms and purposes defined by this Policy, the Operator collects personal data of physical entities which allow or may allow to identify directly or indirectly the personality thereof, including:

- name, surname;
- passport data;
- date of birth;
- contact information (address, email address, phone number etc.)[xxxii].

No information was found about how the company collects that user information, or about the limits of the collection of user information.

In Team Telecom there is only information about data collected from the user - details of the identity document of the given person and/or, if any, the representative of the latter (passport, identification card, military record book, officer's record book or other identity document stipulated by the legislation of the Republic of Armenia), photo, first name, surname, patronymic, place and date of birth, address of registration and / or actual place of residence, phone number, email address. There is also information on 3-rd party sources.[xxxiii]

With regards to the collection of data, Team Telecom highlights the following: "Personal data to be obtained through secondary sources:

- Identity card data: series, number, date of issue, details of the issuing authority, validity period, status (valid, invalid)
- Name, surname, patronymic, photo,
- Date of birth
- Registration address
- Public services registration number,

- Information about this person in the Compulsory Enforcement Service: the existence of enforcement proceedings, the presence of arrest, the date, the amount of property under arrest, and the amount of the obligation.
- Information on the existence of liability in financial institutions, on the amount of the liability.

Secondary sources are, in particular, the operator of the state information system and third parties authorized to collect credit history or conduct a credit assessment (for example, a credit bureau)."[xxxiv]

Related to the limits of collection of the information: “Your personal data will be processed to the minimum volume necessary to achieve the goals set by this Notice, therefore, the personal data already provided by you will not be obtained from secondary sources, and should they be obtained will be distracted.”[xxxv]

In Ucom there is only information about data collected from the user:

- ID details (passport, identification card, military ID, officer ID, or another identity document stipulated by the laws of the Republic of Armenia) of an individual and his/her representative (if any), name, surname (patronymic), place and date of birth, registration and/or actual residence address;
- phone number, and e-mail address.

And information from 3-rd party sources is also underscored.[xxxvi]

Related to the collection of data, there is the following information from Ucom:

The data provided by the user and some data by third parties: the State Information System Operator, and third persons authorized to collect credit history or to assess creditworthiness (such as credit bureau) for obtaining personal data from databases containing users' personal data.[xxxvii]

Related to the limits of collection of the information: “As far as we will process Your personal data in the minimum quantity necessary for fulfilling the purposes stipulated in Section IV, the personal data received from You will not be obtained from secondary sources.”[xxxviii]

All 3 companies are not providing any information about technical data (like IMEI, IP addresses, visited websites, etc.) and data from 3rd party sources.

As for the sharing of users' information (Indicator P4) Viva-MTs again provides very little information with general references to the legislation: “The personal data of Subscribers may be transferred by Operator to third parties (including outside Armenia) and proceed by them according to the procedures and in cases defined by the RA legislation in force".[xxxix] Related to sharing information with the government, there is only very general information provided: "Very general information: comply with demands or requests made by regulators, government, courts, and law enforcement authorities”.[xl]

Team Telecom is disclosing general information about possible third parties: “We may provide your personal data (exchange personal data) for the purposes established by this Notice, and only to the extent that justifies those purposes:

- to the operator of the state information system;
- to partners, suppliers involved in the provision of services or conducting research on the activities of the Company, and to service providers;

- to third parties who process, store personal data and provide information regarding the fulfillment of obligations of debtors;
- to third parties who have received from the Company the right to demand the fulfillment of the subscriber's / client's obligations or the right to recover in court;
- to shareholders of the company, subsidiaries, and integrated enterprises, representative offices, and branches;
- to Company agents, dealers, distributors, or other service providers who sell Company goods or services or execute other similar activities;
- to third parties who may use personal data (in particular, phone number, e-mail address) for marketing purposes (which can be expressed in the form of receiving short SMS messages / advertising calls, social surveys, displaying advertisements on the Internet, social networks, etc.). The Subscriber hereby agrees that the Company is not responsible for the legal consequences of the messages mentioned in this clause;
- to third parties authorized to collect credit history or conduct credit or solvency assessments;
- to state bodies determined by the RA legislation".[xli]

Team Telecom also provides minimal details about sharing information with state bodies, merely indicating that state bodies can receive information according to the law.[xlii]

Ucom is providing data about third parties: "For the purposes stipulated in Section IV of this Notice, we may provide Your personal data to the following persons (exchange personal data) only to the extent justified by those purposes and only in case of necessity.

- State Information System Operator for obtaining other data on You defined by this Notice on the basis of the data provided by You;
- third persons carrying out personal data processing, storage, and provision of information on fulfillment of liabilities by debtors;
- third persons having been entitled by Ucom to claim or recover under the judicial procedure the debt accumulated by the Subscriber for the Services provided;
- partners, suppliers, and service providers of Ucom engaged in the provision of services or conducting research relating to the activities of Ucom;
- agents, dealers, distributors, franchisees, or other service providers of Ucom engaged in the sale of Ucom products or services or other similar activities;
- third parties authorized to collect credit history or assess creditworthiness;
- shareholders, representative offices, branches, subsidiaries, and affiliates of Ucom;
- RA state authorities as stipulated by the laws of the Republic of Armenia."xliii

Data about state bodies is just a reference to the legislation: "RA state authorities as stipulated by the laws of the Republic of Armenia."[xliv]

With regards to the retention of information about user (indicator P6), Viva-MTS just reports that "Operator preserves personal data:

- for as long as needed to provide Subscribers with the possibility to use the services they have requested;
- where the subscriber has contacted the Operator with a question or request, for as long as necessary to allow the Operator to respond Subscriber's question or request;
- During the period of retention of the documents (archiving period) which contain the personal data of the Subscriber;
- For any other period specified by the RA legislation in force."[xlv]

Team Telecom puts it this way: “We regularly review the terms of storage of personal data in accordance with the requirements of the current legislation of the Republic of Armenia and the Policy adopted by the Company. Your personal data will be stored in accordance with the terms established by the procedures of the Company and in accordance with the legislation of the Republic of Armenia”.[xlvi] And in relation to the destruction of data, we are informed that: “TELECOM Armenia” CJSC processes only personal data that are subject to storage in accordance with the legislation of the Republic of Armenia, and personal data necessary to achieve the goals defined by this Notice, avoiding duplicate processing as much as possible. The rest of the personal data is subject to destruction.”[xlvii]

Ucom, similar to other operators, is also providing quite general information with references to the legislation: “We periodically review the periods of retention of personal data in accordance with the requirements of the current legislation of the Republic of Armenia and the Company's policy. Your personal data will be kept in our systems for the duration stipulated by Ucom's procedures and the laws of the Republic of Armenia.”[xlviii]

In the case of users' control of his/her data Viva-MTS again provides data about subscriber's rights regarding personal data: “In terms and purposes of this Policy, the Subscriber may be entitled to:

- ask for access to the personal data Operator holds about him/her;
- request the correction and/or deletion of his/her personal data;
- request the restriction of the processing of his/her personal data, or object to that processing;
- withdraw the consent to the processing of his/her personal data (where the Operator is processing Subscriber’s personal data based on his/her consent);
- complain to the local data protection authority if his/her privacy rights are violated, or if he/she has suffered as a result of unlawful processing of personal data.”[xlix]

Team Telecom is providing less information, referring to the legislation:
“You have the rights determined by the RA Law “On the Protection of Personal Data.”

You have the right to withdraw your consent to the processing of personal data or to request the deletion of your personal data. However, in this case, unfortunately, we will not be able to continue to provide you with the Services. In addition, it should be noted that the deletion of personal data due to legal requirements, other obligations, and factors is not always possible.” [l]

Information provided by Ucom is very general: “You have the rights enshrined in the Law of the Republic of Armenia “On Personal Data Protection”. You have the right to withdraw Your consent to the processing of personal data. In this case, however, we cannot continue to provide Services to You.”[li]

Companies are not openly disclosing information related to how users can access their own information (indicator P8), how companies respond to governmental (indicator P10(a)), private (indicator P10(b)) requests. There is no information on how companies are dealing with possible data breaches (indicator P15). We don't have any information about the usage by companies of algorithmic systems.

Conclusion

Overall, operators tend to provide vague terms of service and privacy policy without delving into specifics. Companies should provide more detailed terms of service and privacy policy to their customers. They should be transparent about how they collect and use personal data, and with whom they share it.

They often reference Armenian legislation to avoid providing concrete information. Companies should provide precise information about their data protection strategies and not solely rely on references to Armenian legislation.

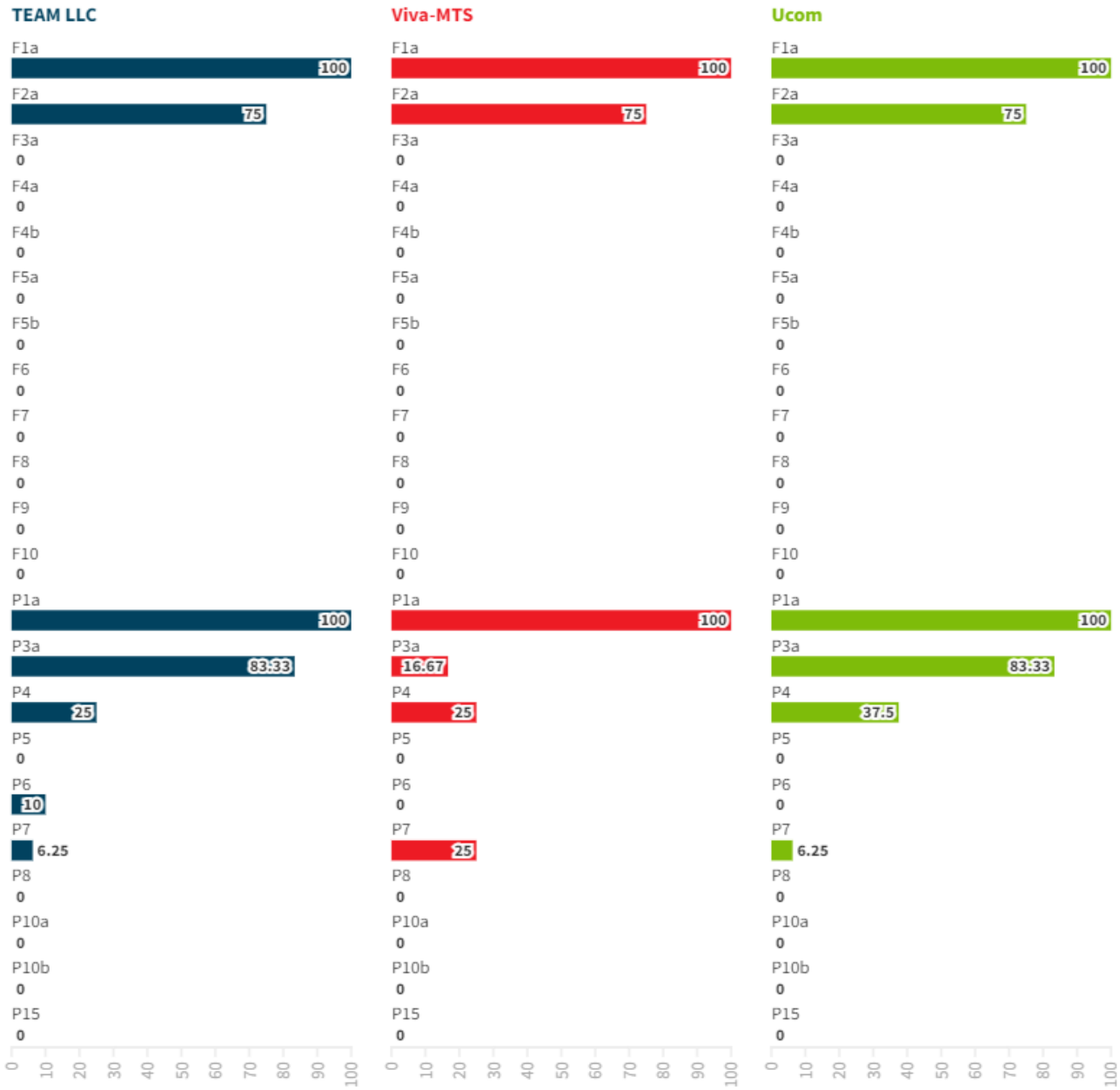
However, the legislation itself is not particularly specific when it comes to personal data and governmental requests to private companies. Armenian legislation should be revised and updated to provide more specific guidelines on personal data protection. This will help close the gaps that could potentially enable the misuse of personal data and other human rights violations.

The State Data Protection Agency should be more proactive in monitoring and enforcing data protection policies and regulations, especially in the telecom sector. This will ensure that operators comply with the laws and regulations and protect consumers' privacy rights.

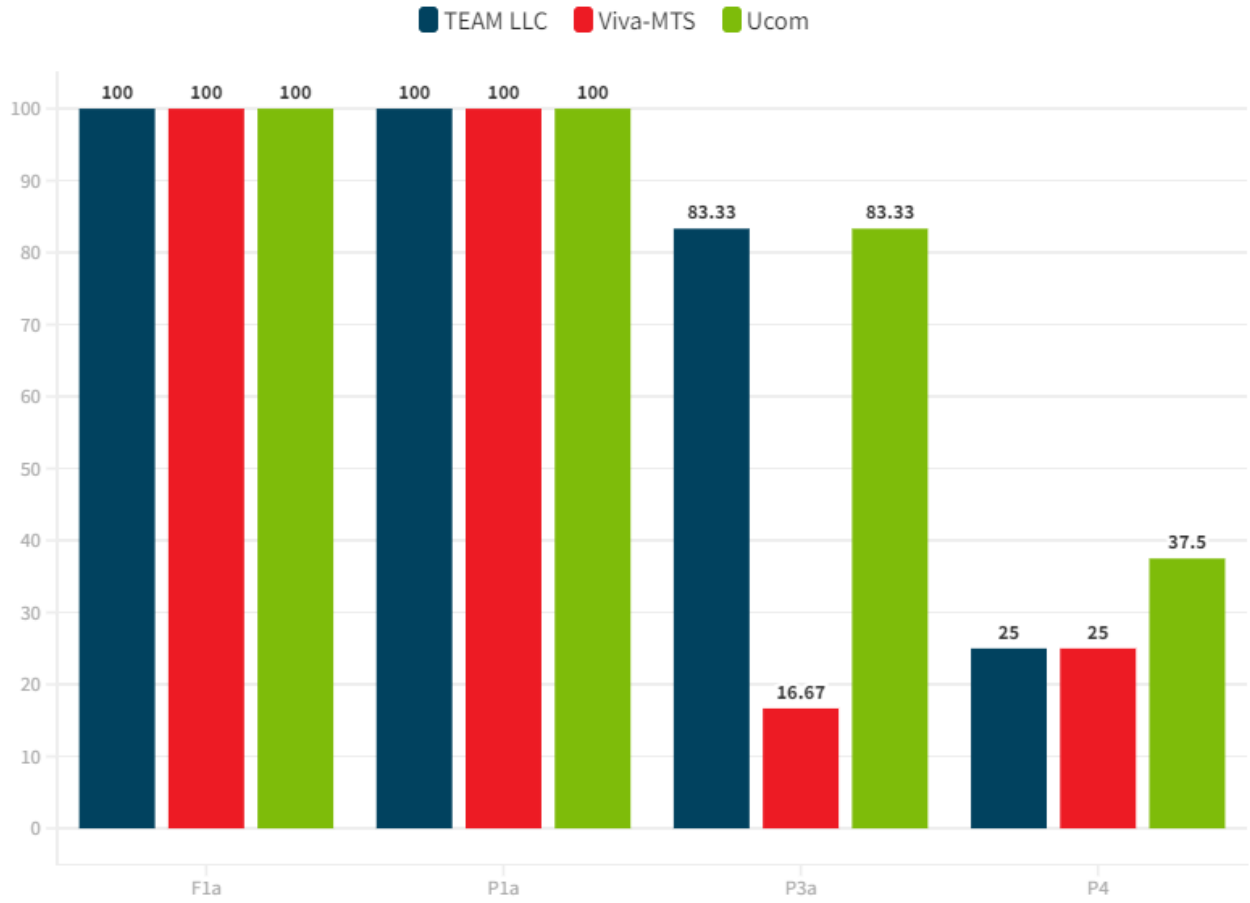
Additionally, educational programs should be conducted to raise public awareness about data protection, privacy rights, and the risks of sharing personal data online. This will help consumers make informed decisions about sharing their personal information with operators as well as be more proactive about demanding information and transparency about their data protection and sharing practices.

Appendix

Indicators. Ranking Digital Rights



Main Indicators Compared. Ranking Digital Rights



[i] PSRC regulates industries in Armenia including electricity, natural gas, water, and electronic communications. https://psrc.am/

[ii] 2008 Armenian presidential election protests https://en.wikipedia.org/wiki/2008_Armenian_presidential_election_protests

[iii] Main Armenian state intelligence agency with very wide duties and capacities https://en.wikipedia.org/wiki/National_Security_Service_(Armenia)

[iv] The Impact of March 1st on the Field of Armenian Media, Samvel Martirosyan, https://media.am/en/critique/2018/03/06/9401/

[v] Armenia Freedom On The Net report, 2017, https://freedomhouse.org/country/armenia/freedom-net/2017

[vi] TikTok fails to operate in Armenia, October 01, 2020, https://armenpress.am/arm/news/1029718.html

[vii] "Main problems of Internet freedom in Armenia [in Armenian]," Media.am, January 18, 2021, https://media.am/hy/critique/2021/01/18/25891/.
Armenia Freedom On The Net report, 2021, https://freedomhouse.org/country/armenia/freedom-net/2021

[viii] Freedom House Condemns Azerbaijani Attacks on Armenia, Calls for Diplomacy, https://freedomhouse.org/article/freedom-house-condemns-azerbaijani-attacks-armenia-calls-diplomacy

[ix] https://twitter.com/Kornelij/status/1573251601518804992

[x] The Cyber Battlefield is Just as Important: Armenia's Cybersecurity, January 27, 2021, https://evnreport.com/magazine-issues/the-cyber-battlefield-is-just-as-important-armenia-s-cybersecurity/

[xi] The Law on Protection Of Personal Data http://www.foi.am/u_files/file/Personaldataprotectionlaw_ENG.pdf

[xii] Coronavirus Phone Tracking Launched In Armenia, April 17, 2020, https://www.azatutyun.am/a/30540411.html

[xiii] Armenia: Security Concerns Raised About the Computer Program Tracking the Movement of Coronavirus Carriers, May 7, 2020, https://hetq.am/en/article/116810

[xiv] "Statement on the destruction of information and storage devices [in Armenian]," Government of Armenia, September 25, 2020, https://www.gov.am/u_files/file/Haytararutyunner/Ardzanagrutyun.pdf.

[xv] Exclusive: Armenia's biggest mobile phone operator up for sale, October 10, 2022, https://www.civilnet.am/en/news/678515/exclusive-armenias-biggest-mobile-phone-operator-up-for-sale/

[xvi] B24.am (2022). Number of mobile subscribers in Armenia [online] Business 24. Available at: https://b24.am/business/340934.html [Accessed 1 Mar. 2023]
[xvii] Details of the 2020 RDR Index methodology are available:https://rankingdigitalrights.org/2020- indicators
[xviii] Details of the 2020 RDR Index methodology are available: https://rankingdigitalrights.org/2020- indicators/
[xix] General Terms of Provisioning Mobile Electronic Communication Services https://www.mts.am/en/more/legal-information/general-terms-of-provisioning-mobile-electronic-communication-services
[xx] Privacy Policyhttps://www.mts.am/en/more/legal-information/privacy-policy
[xxi] General Terms And Conditions For The Provision Of Electronic Communication And Other Serviceshttps://www.telecomarmenia.am/file_manager/terms_and_conditions/terms_and_conditions_en.pdf
[xxii] https://www.telecomarmenia.am/en/privacy-policy/
[xxiii] General Terms And Conditions For Provision Of Electronic Communication And Other Related Services https://www.ucom.am/file_manager/gtc/2022/GTC%20_Final%20version_ENG_07.03.2022.pdf
[xxiv] Personal Data Processing Policy/ Notice On Personal Data Processinghttps://www.ucom.am/file_manager/poa/20190603_UCOM_privacy%20policy(en)_ENG.pdf
[xxv] 14.8 of General Terms of Provisioning Mobile Electronic Communication Services https://www.mts.am/en/more/legal-information/general-terms-of-provisioning-mobile-electronic-communication-services
[xxvi] 18.5 of General Terms And Conditions For The Provision Of Electronic Communication And Other Serviceshttps://www.telecomarmenia.am/file_manager/terms_and_conditions/terms_and_conditions_en.pdf
[xxvii] 17.7 of General Terms And Conditions For Provision Of Electronic Communication And Other Related Services https://www.ucom.am/file_manager/gtc/2022/GTC%20_Final%20version_ENG_07.03.2022.pdf
[xxviii] Tariff types with 0 rates for the different services of Team Telecom https://www.telecomarmenia.am/en/mobile-tariffs/, Ucom https://www.ucom.am/en/personal/personal-mobile-services/voice-prepaid/prepaid-levelup/, Viva-MTS https://www.mts.am/en/individual-customers/mobile-network/tariffs-and-discounts/x-y-z-tariff-plans/for--prepaid
[xxix] Privacy Policyhttps://www.mts.am/en/more/legal-information/privacy-policy
[xxx] Privacy Policyhttps://www.telecomarmenia.am/en/privacy-policy/
[xxxi] Personal Data Processing Policy/ Notice On Personal Data Processinghttps://www.ucom.am/file_manager/poa/20190603_UCOM_privacy%20policy(en)_ENG.pdf
[xxxii] A section of the Privacy Policy https://www.mts.am/en/more/legal-information/privacy-policy
[xxxiii] 4 section of Privacy Policyhttps://www.telecomarmenia.am/en/privacy-policy/
[xxxiv] 4 section of Privacy Policyhttps://www.telecomarmenia.am/en/privacy-policy/
[xxxv] 4 section of Privacy Policyhttps://www.telecomarmenia.am/en/privacy-policy/
[xxxvi] III section of Personal Data Processing Policy/ Notice On Personal Data Processinghttps://www.ucom.am/file_manager/poa/20190603_UCOM_privacy%20policy(en)_ENG.pdf
[xxxvii] III section of Personal Data Processing Policy/ Notice On Personal Data Processinghttps://www.ucom.am/file_manager/poa/20190603_UCOM_privacy%20policy(en)_ENG.pdf
[xxxviii] III section of Personal Data Processing Policy/ Notice On Personal Data Processinghttps://www.ucom.am/file_manager/poa/20190603_UCOM_privacy%20policy(en)_ENG.pdf
[xxxix] D section of Privacy Policy https://www.mts.am/en/more/legal-information/privacy-policy
[xl] B chapter of Privacy Policy https://www.mts.am/en/more/legal-information/privacy-policy
[xli] 7 chapter of the Privacy Policyhttps://www.telecomarmenia.am/en/privacy-policy/
[xlii] 7 chapter of Privacy Policyhttps://www.telecomarmenia.am/en/privacy-policy/
[xliii] IVsection of Personal Data Processing Policy/ Notice On Personal Data Processinghttps://www.ucom.am/file_manager/poa/20190603_UCOM_privacy%20policy(en)_ENG.pdf
[xliv] VI chapter, 8th point of Personal Data Processing Policy/ Notice On Personal Data Processinghttps://www.ucom.am/file_manager/poa/20190603_UCOM_privacy%20policy(en)_ENG.pdf
[xlv] C) Terms of processing of personal data of Privacy Policy https://www.mts.am/en/more/legal-information/privacy-policy
[xlvi] 8. Terms of storage of personal data of Privacy Policyhttps://www.telecomarmenia.am/en/privacy-policy/
[xlvii] 9. Destruction of personal data of Privacy Policyhttps://www.telecomarmenia.am/en/privacy-policy/
[xlviii] V. How long are Your data retained? Personal Data Processing Policy/ Notice On Personal Data Processinghttps://www.ucom.am/file_manager/poa/20190603_UCOM_privacy%20policy(en)_ENG.pdf
[xlix] F) Subscriber's rights regarding personal data of Privacy Policy https://www.mts.am/en/more/legal-information/privacy-policy
[l] 10. Your rights of Privacy Policyhttps://www.telecomarmenia.am/en/privacy-policy/
[li] VIII. Your rights. Personal Data Processing Policy/ Notice On Personal Data Processinghttps://www.ucom.am/file_manager/poa/20190603_UCOM_privacy%20policy(en)_ENG.pdf