MTX Connect S.á r.l.
37 Grand rue
Pontpierre, L-4393, Luxembourg

To: Body of European Regulators for Electronic Communications
BEREC-WP-2022@berec.europa.eu

5 November 2021

Re.: Public consultation on the BEREC Work Program 2022

Dear Madams, Sirs,

MTX Connect S.à r.l. (**MTX**) is a full MVNO, established in Luxembourg in 2013. Within the scope of the BEREC Work Program 2022 we would like to raise the BEREC's attention to several subjects. Those are matters that MTX, just like other small operators and MVNOs, encounters when trying to get regulated access to networks and services across Europe. Some of them are persistent throughout a number of years and despite the continuous BEREC's attempts to mitigate the constrains through opinions and guidelines. Others are occasional but still worth paying attention to.

In particular, the difficulties we experience concern: general authorization, access to networks and interconnection services, wholesale roaming access, some aspects of regulated roaming, such as definition of fair use in roaming agreements and diverse approaches of operators to identification of regulated traffic. In addition to that, we would like to express our opinion on the ambiguities in application of data protection laws in telecoms sector. As a separate query, we would like BEREC to clarify certain aspects of caller location identification obligations in case of emergency communications.

1. <u>General authorization.</u>

National regulatory authorities (**NRA**) in some member states insist on presenting by the MVNO applicants of an MVNO agreement at the stage of general authorization and provision of rights to use the national numbering plan. Neither the Authorization Directive, nor the EECC contain any incentive for the NRAs to require from the applicant to prove its ability to render the electronic communications services. BEREC guidelines on the notification template[1], issued back in December 2019, are also silent on this matter.

The law allows NRA to check only the minimum information about the applicant. The purpose of collecting the information about the applicant is to maintain a register of operators. Therefore, a demand for information must be proportionate and objectively justified. The minimum information comprises a short description of network and services and the respective charges and fees. In case of request for use the numbering resources such information is needed to assess the request but there is no legal requirement to prove the ability of the applicant to render the communications services.

[1] BoR (19) 259

In our opinion, demanding the presentation of an MVNO agreement goes far beyond the criteria of proportionality and objectiveness.

A demand for MVNO agreement at the general authorization stage puts an applicant into a difficult situation. The applicant is likely a newcomer in telecoms sector or a small MVNO from another member state, willing to have its own numbering resources in a given country in order to render the communications services. Such undertaking unlikely has any administrative, financial and especially timing capacity to appeal the NRA requirement for MVNO agreement. What it can do is to find a local MNO that would agree to sign the required MVNO agreement or a memorandum of understanding or any other similar document. And here MVNO faces several difficulties:

(a) No MNO may wish to start any negotiations with an entity that is not duly authorized provider of electronic communications services. So, it is already a deadlock;

(b) Local MNOs may not wish to negotiate any such agreement at all simply because they do not want to deal with MVNOs. There is no general obligations for MNOs to do it;

(c) Suggestion to sign a nonbinding document may be rejected by MNO for the same reasons mentioned above;

(d) MVNO agreement may contain exclusivity provisions that deprive the respective MVNO from entering other markets or negotiating with other local MNOs, or it may contain other detrimental terms that MVNO can be forced to accept simply because NRA requires a signed MVNO agreement;

(e) NRA may not accept a nonbinding document (such as MOU or LOI, etc.) as a substitution to a regular MVNO agreement;

(f) Depending on the chosen business model, MVNO may not need the rights to use local numbering plan and thus no need to have an MVNO agreement at all with local MNOs. However, even at the stage of the notification for general authorization an MVNO applicant might be forced to have such agreement anyway.

In our opinion, NRAs exceed their competence when they request for MVNO agreement at the stage of the general authorization (including the requests for right to use the numbering resources). Such demand impairs the market position of the applicant and jeopardizes the objectives of the EU telecoms regulation with respect to development of the internal market.

One of the NRAs that requires the MVNO agreement for provision of rights to use the numbering plan is Cyprus NRA.

2. Access to networks and interconnection services.

We divide this section into subsections since there are several hurdles that an MVNO may experience with respect to request for access to networks and interconnection services.

2.1. Transparency.

Obligation of transparency aims to speed-up the negotiations and to ensure the interoperability. An access provider may be obliged to publish its reference offer for access and/or interconnection, which shall be sufficiently detailed with respect to offered products and services and the respective fees and charges. At the same time, BEREC guidelines on the minimum criteria for a reference offer[2] allow the access providers to restrict the access to certain elements of or to the entire reference offer "for security reasons". The restriction is allowed subject to NRA's decision on the matter. This approach seems to undermine the aim of the transparency principle.

What happens in practice? The access seeker does not know whether there is a reference offer published by a certain operator. Because operators do not make available neither the reference offer itself, nor any information about its existence, nor any restrictions on publishing thereof allowed by the NRA. In some cases, the reference offers are published in website sections lacking any pointing hyperlinks, so the access seeker cannot find them. Internet search does not lead to the required offer. NRAs do not inform the access seekers about any publishing restrictions allowed with respect to reference offers.

On the other hand, even if there are no publishing restrictions the situation is the same. NRAs do not check to what extent the transparency obligation is observed. Obliged operator sends to its NRA a link to a certain website where the NRA may find and check the offer. However, this link is not indexed in internet searches, it does not lead to the respective operator's publicly visible and easily accessible website.

We invite BEREC to randomly check the public availability of reference offers of operators that are obliged to do it, with and without any publishing restrictions allowed by their NRAs. In the majority of cases, it would be highly difficult if not impossible to find. The same concerns the respective NRAs; they do not provide any information on their websites about restrictions allowed to their operators with respect to publishing the reference offers.

What an access seeker can do is to directly request the access provider for its reference offer. This opens an opportunity for the access provider to ignore such request.

This query was discussed with one of the BEREC representatives during the Stakeholders' Forum 2021 in Brussels. The BEREC representative supported the position of access providers in hiding their offers and relied on the security matters that may arise if an access provider publicly makes available the locations of its facilities involved in the provision of services under the respective reference offer. This argument seems insufficient to justify the non-observance of transparency obligation. The minimum information that must be covered in the reference offer include the description of

[2] BoR (19) 238

networks and services, respective terms and conditions and prices. It appears reasonable not to publish the sensitive parts of the offer and to leave it for further negotiations between the parties, but not publishing the reference offer at all does not serve the objectives of the EU telecom regulations.

2.2. Reasonableness.

Regulatory obligation to meet reasonable request for access to, and use of, network and interconnection services creates ambiguities with respect to identification of reasonability criterion. There are maximum Union-wide mobile termination rates in place but other costs that access provider may require access seeker to cover remain subject to commercial negotiations. Addressing this issue to NRAs is fruitless. NRAs are not willing to assess to what extent the network access and interconnection request are reasonable from the access provers' perspective. It means that access providers are free to impose unregulated commercial terms on their regulatory obligations.

The idea of good faith negotiations does not cover the period of negotiation. At least the access providers refuse to consider reasonable negotiation period as a part of good faith negotiation requirement. And the law does not contain any reference to reasonability of period of negotiations. Appealing to NRAs in case where access provider postpones negotiations for no reason does not resolve the situation. NRAs often refuse to force access providers to expediate the negotiation process.

2.3. Withdrawal of already granted access.

It is unclear how the requirement not to withdraw the already granted access correlates to a contractual right to terminate the agreement. A similar problem that happened under the regulated roaming regime will be exemplified in section 3.3 below.

What an access seeker can do if the access provider insists on having a contractual right to terminate the contract? Such right allows the access provider to terminate the contract as soon as it is signed, which will force the access seekers to go all over the same negotiation process again Unlike in regulated roaming relations, an access to networks and services has no regulated time periods for negotiations. In other words, there is a risk of abuse of contractual rights with the purpose to avoid or considerably postpone the performance of operator's regulatory obligations.

This issue concerns all regulated access obligations.

3. Wholesale roaming access.

3.1. Transparency.

The issues described in section 2.1 above with respect to making available the reference offers apply to the regulated wholesale roaming access reference offers to the same extent. The Roaming Regulation explicitly requires the access providers to "publish [and] make it available"[3] to access seekers, but still a great number of operators across the EU

[3] Roaming Regulation, art. 3.5

obfuscate their wholesale roaming access offers from public. A random check on operators' websites may exemplify how operators of the same member state or operators of the same international group differently interpret the obligation of transparency.

However, it must be admitted that the situation with publicly available and easily accessible wholesale roaming access reference offers is much better than for general access to networks and services. We have not undertaken a deeper analysis on this matter and cannot say whether there is any correlation between the operators from net sending and sent receiving member states and their intention to hide their offers from public and whether there are other reasons not to make the reference offers public. It would be interesting to have a separate study on this matter.

3.2. Access through unregulated entities.

It is a common business practice to concentrate a particular business activity in one hand, be it a department within the same undertaking or a separate special purpose entity (**SPE**). It saves costs and increases the productivity and efficiency. Besides, from the access seeker's perspective an access through such SPE may increase the network coverage if that SPE represents several operators from different regions. A publicly known example of dealing through SPE is Vodafone[4]. Vodafone companies and Vodafone partners delegate their roaming arrangements to a SPE based in Luxembourg, Vodafone Roaming Services S.à r.l. Even the regulated wholesale roaming access arrangements are dealt through this SPE.

However, there are certain pitfalls in this business model that affect the operators' obligations to meet reasonable requests for access and the corresponding rights of access seekers. The problem in the given example of Vodafone SPE is that despite the fact that this SPE states its NACE code in Luxembourg Trade and Companies Register as 61.200 *Wireless telecommunications activ*ities[5], it appears that it has never filed a notification with Luxembourg NRA for the general authorization within the EU telecom laws. At least the Luxembourg NRA does not list this entity in its register of authorized operators[6]. We are not aware whether this particular Vodafone SPE has filed any notification for general authorization in other member states, but for the Luxembourg NRA this entity is an unregulated undertaking within the EU telecoms' framework. This situation creates certain ambiguities for the access seekers.

First, unregulated SPE is not bound by the regulated obligations. Potentially it poses questions about transparency and non-discrimination with respect to access seekers. Nothing prevents an SPE to alter the operator's reference offer or to impose additional terms and conditions that may undermine the commercial value of the access sought. It is not clear whether the SPE applies similar conditions to equivalent transactions or not.

---

[4] https://www.vodafone.com/about-vodafone/where-we-operate/roaming-services?utm_source=google&utm_medium=cpc&utm_campaign=vrs_general

[5] https://www.lbr.lu/mjrcs/jsp/DisplayConsultDetailCompanyActionNotSecured.action?time=1635950883450&CURRENT_TIMESTAMP_ID=1635950878706#null

[6] https://web.ilr.lu/FR/Professionnels/Communications-electroniques/Acces-au-marche/Autorisation/Registre-public/Pages/default.aspx

There might be a potential abuse of competition law restrictions mentioned in articles 101-102 of TFEU as well.

Second, it is unclear how to resolve the disputes over the regulatory obligations of respective operators. This problem has multiple layers. To begin with, it is unclear which NRA shall be involved in such dispute? If the matter concerns the regulatory obligations of only one operator, then presumably the respective domestic NRAs of the access seeker and the operator in question will be involved. In case where the regulatory obligations concern several operators from different member states, then it can be assumed that all their domestic NRAs shall be involved in the dispute resolution process. However, this does not resolve the ultimate pitfall: how an NRA may force an unregulated SPE to perform the regulatory obligations? Only the duly authorized operators may be obliged to perform the obligations laid down on them as a result of a dispute resolution process within the telecoms framework. As a side problem to this issue, the operators delegated their roaming obligations to SPE may claim that they do not have any direct contractual relationship with the access seeker and thus they may refuse to be a party to the dispute.

Needless to say, that NRA of the member state where an SPE is based has no competence to deal with disputes involving such unregulated SPE.

To conclude, outsourcing of regulated obligations to unregulated entities poses considerable constrains for the access seeker on all stages of dealing with such SPE, from negotiating the request for access to resolution of disputes. BEREC opinion on this matter would be much welcomed by access seekers and could be helpful for NRAs as well.

3.3. Termination of regulated access.

There was a case in Germany[7] where an access seeker (it was MTX) requested a clarification from the German NRA whether the wholesale roaming access provider had the contractual right to terminate the regulated access. German NRA decided that despite the regulatory right to terminate the access in case of breach of fair use provisions the operator has the contractual right as well and can terminate the regulated access agreement if the contract contains such right.

In practice it means that access provider may exercise its contractual right to terminate the regulated wholesale roaming access at any time. Access seeker in such case will need to undergo the same access request procedure as mentioned in article 3.5 of the Roaming Regulation. Unlike in general regulated access to networks and services provisions, the Roaming Regulation sets out certain time limits for the access provider to observe: one month to provide a draft contract and to grant the roaming access within maximum three months after the contract is signed. Although, the time period for negotiation of the contract itself is no mentioned, still the access seeker has some approximate timing estimates.

Nevertheless, contractual right to terminate the regulated access gives the access provider an opportunity to delay the provision of roaming services and in some cases to

[7] BNetzA ruling BK2-17-006 of 16 July 2018

require a re-negotiation of previously agreed terms. Access seeker has no protection against such tactics.

4. Permanent roaming, anomalous or abusive traffic use.

With increased convergence of services, it becomes more and more problematic to negotiate and observe the fair use terms in regulated wholesale roaming access agreements.

The notion of stable links to an EEA member state still poses identification problems in border regions where operators apply different methods to calculate the time spent by the end-user in a visited and home network. Some rely on a mere fact that at a given date the respective SIM card is registered in a specific network. Others, to the contrary, take into consideration only the exact time spent by the SIM card in a particular network; but this requires considerable administrative, technical and financial exposure for the operators. As a result, the parties either fall into fruitless negotiations about the regulated traffic detection methods or the access provider simply applies the contractual penalties to the suspicious traffic. MVNOs in this case are always on the losing side.

A particular issue concerns eSIMs. End-users either do not know how to switch off the eSIM so it ceases to be registered in a visited network, or they forget to do it. As a consequence, the operator considers the eSIM to remain in permanent roaming or to represent a "device traffic" (see below) and may block the end-user, not to mention the contractual penalties it may face from the visited operator.

The most problematic becomes any traffic that is not initiated by a human being: IoT, M2M, "device traffic" and all other types of traffic that fall beyond the roam-like-at-home (**RLAH**) concept. Identification of IoT/M2M traffic use through IMEI could be unreliable due to the absence of unified, publicly available, consistent, and error free TAC IMEI databases. Consumption pattern analysis can be extremely costly for the operators because it requires state-of-the-art algorithms that cannot be afforded by small operators and MVNOs, for example. Besides, there are numerous borderline cases where consumption pattern of a human traffic eligible to RLAH looks exactly the same as IoT/M2M traffic and it is impossible to differentiate which one falls under the regulated rates. Consequently, operators with substantial bargaining power (in case where MVNO is the access seeker these will always be MNOs) may apply contractual penalties, claim for abuse of fair use terms and terminate the access. We suppose that a detection of the regulated and anomalous or abusive traffic use will likely become a material problem for the operators in the years to come.

5. Caller location information.

With respect to emergency communications, we have a particular query regarding the provisions of article 109.6 of the EECC on caller location identification (**CLI**). The implementation of CLI is subject to national laws and the Commission delegated acts[8]. The first deadline for such acts is set out for 21 December 2022. BEREC is supposed to

[8] EECC, art. 109.8

provide its opinion on the subject matter. Regarding this obligation we would like to stress the BEREC's attention to the following.

Each member state will have its own rules on compatibility, interoperability, integration, protocols and other matters of the CLI. The general concept is that national operator will provide a respective CLI to a local PSAP in a format and in a way as prescribed by national law. The emergency communications are executed through a local breakout. The question is who shall provide the CLI (if at all) in case of emergency call originated from a SIM card registered in a visited network while roaming? The obligation to comply with CLI requirement falls on the visited operator or remains on the home operator? If it is the home operator then to which PSAP shall it send the CLI? If it shall be sent to the PSAP of a visited country then in what format and through what channels shall the home operator fulfil its obligation: in accordance with its national law or under the rules of the visited member state? In the latter case, how a home operator can be aware of the emergency communications requirements of the visited member state and will such awareness not overcomplicate the CLI obligations for the home operator?

This is a crucial point for all operators and we would very much appreciate the BEREC's expeditious opinion on the matter.

6. Data protection.

Although, data protection falls beyond the BEREC direct competence, there are still some aspects that need clarification from both, BEREC and the European Data Protection Board (**EDPB**). Bearing in mind that pursuant to article 4.7 of the Regulation (EU) 2018/1971[9] and section 4 of the BEREC Work Program 2022 BEREC may cooperate with other EU bodies, we decided to address to BEREC our data protection query as well.

The current EU data privacy framework that applies to electronic communications comprises Directive 2002/58/EC (**E-privacy Directive**) and Regulation (EU) 2016/679 (**GDPR**). Article 95 of GDPR explicitly limits the application of GDPR to the situations which are subject to specific obligations under the E-privacy Directive. Nevertheless, many operators within the EEA and outside Europe insist on having specific data processing agreement (**DPA**) in accordance with standard contractual clauses under the GDPR.

In our opinion, the requirement for DPA in public electronic communications impairs the idea of telecoms industry to convey communications and lays redundant bureaucratic burden on operators. In the majority of cases the requesting party cannot justify its request for DPA. The only argument is that there is a mandatory requirement to have DPA in place; even in situations where there is no potential for data processing whatsoever (such as in interconnection agreements, where only the traffic data can be exchanged, which is covered by the E-privacy Directive and thus is excluded from GDPR under its article 95).

We strongly advise BEREC to raise this issue with EDPB and to produce a join opinion or a guideline with respect to processing of data that is essential for the conveyance of

[9] Article 4.7

electronic communications, including the documents and information confirming the stable links of roaming customers. Otherwise, the lack of clear understanding of diverse data privacy rules undermines the negotiation process between operators and increases the administrative burden and unnecessary paperwork for contracting parties.

7. Conclusion.

In this response to the public consultations on the BEREC Work Program 2022, MTX would like to stress the BEREC's attention to the most critical points that small operators and MVNOs are likely to come across under the current EU telecom framework. Some of these hurdles are persistent for a number of years already, others are popping up while the new regulatory rules evolve. At any rate, each of the issues we listed herein represent a draining experience for operators and considerably impede the achievement of ultimate objectives of the EU telecom regulation, notably with respect to development of the internal market.

We remain open for cooperation with BEREC with respect to additional information or clarification of our concerns raised in this response. Please address your questions and queries to consultations@mtxc.eu.

Sincerely,

MTX Connect S.à r.l.