Office of the
Telecommunications
Adjudicator

Industry Principles for All-IP Migration

Best Practice Guide

Version 2

1. Introduction

This document provides an agreed set of principles to act as a baseline for the development of Best Practice information and supporting processes associated with both the Openreach programme to withdraw WLR and the wider migration to All-IP products across industry; both within and between networks and inter and intra CP.

The objective of these principles is to ensure the protection of the consumer and to minimise customer disruption, especially to vulnerable customers and Critical National Infrastructure. The principles seek to ensure, as far as is practical, service continuity and that customers are not left without a working service or suffer a material impact to critical or life affecting services which rely upon the underlying telecoms product(s).

The principles aim to support both the Ofcom October 2018 guidance regarding Emergency Calls and the Ofcom 2019 Policy Statement covering the wider transition to All-IP.

2. Audience for the Principles

These principles are aimed at all Communications Providers (CP), Network Operators (NO), both existing and new and Wholesalers supporting resale CP channels.

The expectation is that where there is an extended sales chain, Network Operators and Wholesalers will also flow through the requirements and obligations of the principles within their channels to market.

3. Working with OTA2

Signatories commit to working with OTA2 to track and report, as far as is practical, the success of migration activities and the scale and nature of any failures. Signatories also commit to work with OTA2 and other industry parties to;

a) seek resolution to any systemic issues that affect vulnerable customers or CNI and

b) share and communicate best practice across industry, within its organisation and through their channels to market

4. Relevant General Conditions

While not exhaustive, relevant General Conditions (GC) relating to vulnerable end customers within the context of All-IP migration are:

- General Condition A3.2(b) - CPs to "take all necessary measures" to ensure "uninterrupted access to Emergency Organisations as part of any Publicly Available Telephone Services offered" when customers are making calls over broadband.
- GC3.3. - "Regulated Providers must inform their Domestic and Small Business Customers in plain English and in an easily accessible manner that access to Emergency Organisations using VoIP Outbound Call Services may cease if there is a power cut or power failure, or a failure of the internet connection on which the service relies" While the focus of this GC is on outbound VoIP services, the requirement that appropriate information must be provided during the sales process, within the terms and conditions of use, and in any user guide issued by the Regulated Provider is relevant to all digital voice services.
- General Condition on 'Measures to meet the needs of vulnerable consumers and end-users with disabilities' (GCC5) – This includes a requirement that communications providers establish, publish and comply with policies and procedures to ensure that the needs of vulnerable consumers are adequately considered and met. Ofcom stipulate that those policies and procedures must include "how information about the needs of Consumers who the Regulated Provider has been informed or should otherwise reasonably be aware may be vulnerable will be recorded…". Therefore, Ofcom consider that providers should already be considering how to record and retain sensitive information regarding their vulnerable customers in a GDPR compliant way.

5. Communications Providers (CP)

Ofcom have referenced their October 2018 guidance regarding Emergency Calls and 2019 Policy Statement as providing clarity of their expectations of industry in terms of supporting vulnerable and CNI customers. The following is not exhaustive and should be considered only as a summary of the key responsibilities regarding CP support of emergency service access;

- Communication Providers should have at least one solution available that enables continued access to emergency organisations for a minimum of one hour in the event of a power outage in the premises plus;
  - Ofcom consider that both the broadband provider and VoIP provider, if different, should take responsibility for ensuring that their customers are protected and should develop appropriate processes and communications to ensure this
  - When considering whether the solution is suitable for the needs of the customer, Ofcom would expect providers to be giving due consideration to the customer's situation. For example, if the provider is offering a solution which relies on mobile signal to work, then they should ensure that the customer lives in premises that have internal mobile coverage.

  - With regard to talk time, Ofcom consider that providers should ensure that the protection solutions they deploy gives customers sufficient talk time to have a meaningful conversation with the emergency organisations
  - Ofcom expect providers to make clear any limitations of the solution they are offering, for example, if the solution powers the router and permits its usual functionality, customers will need to be aware that using their broadband connection for other applications during a power outage will reduce the amount of time it will support emergency calls.
  - Ofcom expect providers to consider the complexity of any maintenance required for their proposed solution and the capabilities of their customers to support this

- The solution should be suitable for customers' needs and should be offered free of charge to those who are at risk as they are dependent on their landline;
- Providers should take steps to identify at risk customers and engage in effective communications to ensure all customers understand the risk and eligibility criteria and can request the protection solution;
- Providers should have a process to ensure that customers who move to a new house or whose circumstances change in some other way are aware of the risk and protection solution available

In support of the wider move to All-IP, Communications Providers also need to;

- Provide clear and readily available information which informs existing and prospective customers of the potential impacts of the move to All-IP and how they can mitigate these
- Ensure that all customers are given reasonable notice of any managed migration of affecting their services
- Take all reasonable steps to ensure that end customers are fully informed of the potential issues (including impact on telecare and other safety-of-life services) which may result from a migration to All-IP. This should include the use of the appropriate scripts to identify whether any person at a premises is vulnerable or at risk from any disruption to their communication services including whether any additional equipment utilises the existing PSTN line. Where such equipment is identified, end users must be clearly advised that they need to contact their equipment supplier as a matter of priority and preferably given guidance on how this might be undertaken, such as by advising them to press their pendant to reach their Alarm Receiving Centre. Similarly, acquisition of new customers should include asking customers if they use safety of life equipment and the provision of appropriate advice during the sales process CPs should also communicate what additional help is available from the themselves (and any limitation to this) to help support migration, such as home visits, co-op with service provider etc.
- Ensure that where additional equipment, vulnerability or the need for extra support is identified at the point of sale that the provision/migration date allows reasonable time the end user to arrange for any 3rd party supplier to visit the premises to reconfigure existing equipment in preparation before the migration of service happens. However, this date should also reflect the level of prior notice, severity of impact and flexibility of migration date etc. Where an end-user or their Service

Provider request a reasonable extension to the delivery date, in support of delivering the final solution, CPs will support this where feasible.

- Maintain appropriate procedures for home visits during any intensive migration campaign to avoid the risk of harm to consumers and especially vulnerable customers.
- Ensure clear, effective and rapid escalation processes in place to identify and support vulnerable customers impacted by any migration and that these CP processes dovetail with Network Operator/Wholesaler processes so that they function smoothly across the supply chain
- CPs should ensure that post any move to All-IP, ongoing protection is in place to address any adverse change in customer circumstances

Where relevant, CPs should make downstream service providers aware of any available testing facilities or facilitate access to the facilities offered by network operators, so they can determine whether their services will work effectively over an IP network. CPs will also support industry level engagement of key service providers to help critical users understand and prepare for the move to All-IP.

A CPs business customers will vary in terms of size and complexity but CPs in this market should use reasonable endeavours to undertake a structured approach to identifying the need of the business end customer and especially CNI customers, given the potential impact of the move to All-IP on their CPE. This should also include an understanding of the business customer’s migration requirements “in and out” of normal working hours.

6. Network Operator and Wholesaler commitment to Ofcom Requirements

While Network Operators and Wholesalers do not have a direct relationship with the end customer, they should be proactive in seeking to ensure that their channels understand they have a duty of care to proactively inform their end customers about any potential impact associated with the change to their existing telephony services associated with any migration to All-IP.

While the ultimate responsibility lies with the customer facing CP, Network Operator (NO) and Wholesale signatories commit to:

- Clearly highlighting and reinforcing the responsibilities of the customer facing CP in their communication, support material, best practice guides etc. provided to their channels to market
- Being clear as to the support they provide to support the customer facing CP to assist with the fulfilment of the CP’s obligations e.g.
  - Where appropriate working with 3rd parties to support compatibility testing of CPE
  - Whether the Network Operator /Wholesaler can supply and/or support the installation of Battery Back-Up equipment (or an alternative valid solution) or whether this should be sourced by the CP
  - On roll-back to TDM in the event of an issue affecting a vulnerable customer but subject to reasonable considerations such as prior service (i.e. invalid for FTTP to FTTP migration) and infrastructure availability (i.e. switch closure)

- Providing Best Practice Guidance for their channels covering at least:
    - CP obligations
    - Principles and Behaviour
    - Communication with end customer
    - Dealing with vulnerable customers, including roll back or mitigation
    - Approach to Critical National Infrastructure customers
- Ensuring that at any point in the provision/migration journey, an end customer or the supplying CPs have the ability to postpone the migration/order journey and rearrange for a reasonable later date provided this does not jeopardise any previously communicated plans to withdraw the underlying infrastructure. Such reasonable postponement is as to allow time for the resolution of any potential issues that might risk harm to an individual or significantly disrupt a business.
- Working cross-industry to support a capability for rapid restoration of the former communications service in the case of failure of telecare and other safety-of-life services. Such restoration may be time limited due to the availability of the underlying infrastructure.
- Supporting CPs to engage with local and national stakeholders, including CNI organisations, from an early stage to ensure they are aware of any potential implications of a move to All-IP and how to mitigate these.

7. Migration Failures

All parties should have dedicated contact points (for industry consumption only) and supporting processes to help resolve any issues affecting vulnerable individuals and CNI where a service has not migrated successfully.

Where there has been a problem with the provision or migration order and it is identified that the end customer has lost connectivity to their specialist equipment, such as heath pendants or other safety of life services the signatories should provide clear guidance to their channels on the steps to take to ensure they mitigate any harm.

Signatories will seek to work collaboratively to the best effect to reconnect the customer, or otherwise support them in moving to a suitable telephony service.