ANNEX no. 3

Instructions for completing the form for reporting incidents that affected the security and integrity of electronic communications networks and services

<table>
<tr><td colspan="2">1. Provider</td></tr>
<tr><td colspan="2">To be filled in with the name of the provider sending the report to ANCOM.</td></tr>
<tr><td colspan="2">2. Date and hour</td></tr>
<tr><td>2.1 Date and hour when the incident occurred</td><td rowspan="2">To be filled in with the date and hour when the incident occurred, respectively when the incident was detected. The format of introducing the date will be dd.mm.yyyy.</td></tr>
<tr><td>2.2 Date and hour when the incident was detected</td></tr>
<tr><td colspan="2">3. Incident impact and cause type</td></tr>
<tr><td colspan="2">3.1 Affected service/services:</td></tr>
<tr><td colspan="2">There will be checked the service/services whose provision was affected by the incident.
The field ”Number of affected connections” for each service type will be filled in accordingly, the number of connections affected by the incident being specified for each affected service.
A connection is:
- for internet access services provided at fixed locations: an internet access connection;
- for data transmission services provided at fixed locations: an access connection to data transmission services;
- for telephone services provided at fixed locations: a telephone line allotted to a subscriber by a provider through its own fixed network or through a third party’s fixed public network; a subscriber may have one or several access lines;
- for telephone services, internet access and data transmission services provided through land mobile networks: an active SIM card;
- for services of retransmission of linear audiovisual media programmes: an audiovisual programme retransmission connection.
For the services provided by means of public land mobile networks, a provider will estimate the number of affected connections. The method of estimating the number of SIM cards affected by an incident is the following:
When an incident occurs, the number of affected cells will be identified.
The total traffic lost for all the affected cells (T_{lost}) for each service (voice and data) will be deemed to be the traffic registered in the previous week, during the same time interval when the incident occurred, for the respective cells.
The total traffic registered on the network ($T_{network}$) is deemed to be the amount of traffic on all the cells of the network within the respective time interval, during the previous week.
The number of affected SIM cards will be calculated as follows:
$$N_{\text{affected SIM cards}} = N_{sd} \frac{T_{lost}}{T_{network}}$$
N_{sd} is the number of active SIM cards for the respective service, according to the reporting based on the Decision of the President of the Authority for Management and Regulation in Communications no. 333/2013 on reporting statistical data by the providers of public electronic communications services or of publicly available electronic communication services.
In calculating the traffic, one takes into account both the originated and the terminated traffic. The proposed algorithm will be applied to all the types of services provided at mobile locations.</td></tr>
<tr><td colspan="2">3.2 Impact parameters:</td></tr>
<tr><td>Total number of connections affected by the incident</td><td>Here will be specified the total number of connections affected by the incident. This number will be calculated as a sum of the number of connections affected for each type of service.</td></tr>
<tr><td>Affected assets/equipment</td><td>There will be specified the assets/equipment affected by the incident. For example, here is a list of the assets that could be affected:
- PLMN base stations (BSC, BTS, RNC, NodeB etc.);</td></tr>
</table>

	- local network (copper wires, fibre etc.); - street cabinets; - switching or routing equipment (networks switches, routers, multiplexers etc.) - transmission nodes; - switching centres; - message centres; - user registers (HLR, VLR, AuC, Home Subscriber Server etc.); - backbone; - interconnections; - equipment for backup supply of electric power (batteries, generators); - power supply systems.
Incident duration	There will be specified the time interval from the moment when the service started degrading or was interrupted, until the moment when it was provided at a performance level equivalent to that preceding the occurrence of the event. Time will be expressed as minutes.
Area/geographic spread	The geographic region affected by the incident will be specified (e.g.: region, counties, localities).
Impact on emergency calls	There will be specified the manner in which communications to the Unique National System for Emergency Calls were affected.
3.3 Incident description:	
There will be provided any information and details available regarding the incident occurrence, development, impact and manner in which the assets/equipment were/was affected.	
3.4 Type of incident cause:	
The incident causes will be checked: human error, system error, natural phenomenon, malicious action and external cause/third party. Usually, the category external cause/third party may be correlated with one of the other 4 causes (e.g.: in the event of a optical fibre destroyed following some construction works, the incident causes will be human error and external cause/third party). Certain incidents may have an initial cause and a subsequent one, incidents being the result of a sequence of events and factors (e.g.: for an incident occurred following a faulty electricity supply – an overload that triggers a breakdown of the provider's equipment, the initial cause is a system error of a utilities provider's equipment and an external cause/third party, while the subsequent cause is a system error – hardware fault of an electronic communications equipment). In this case, the provider will check the initial cause.	
3.5 Other information on the incident cause:	
This field will specify a detailed description of the incident cause, including the exploited vulnerabilities. For the incidents occurred following a sequence of events, the provider will provide both details regarding the initial cause, and the subsequent cause/causes.	
4. Other information on the incident	
4.1 Incident response actions (including the moment when they were taken):	
This field will provide a detailed description of: - the security measures implemented up to the moment of incident occurrence in order to to minimise the incident risk; - actions taken and measures adopted to provide the services at a performance level equivalent to that preceding the occurrence of the event when the incident affects just the service quality (there is no interruption in the service provision); - actions taken and measures adopted in order to bring the service back to a reasonable level, as well as in order to provide the service at a performance level equivalent to that preceding the occurrence of the event in case of interruption of the service provision, including the moments when these were performed.	

4.2 Measures taken or planned in order to prevent the occurrence of a similar incident / remove the incident cause (including the moment when they have been / will be taken):
The field will comprise the detailed description of the actions taken in order to minimize the risk level and to prevent the re-occurrence of the incident (e.g.: review of security measures and procedures, SLA renegotiation, instructing the personnel, backup equipment or systems acquisition etc.), as well as the moment when these measures were or are to be taken.
4.3 Other providers of electronic communications networks and services affected:
This field will be filled in with details about the provider and its assets/services affected by the respective incident, including the cases when providers from another Member States of the European Union were affected. Moreover, the collaboration with other providers for the purpose of solving the incident, including the common incident response actions will be mentioned.
4.4 Other remarks:
This field will be filled in with further details or remarks that were not mentioned in the fields above.