**3GPP TSG SA WG 1 Meeting #104 S1-23xxxx**

**Chicago, USA, 13 - 17 November 2023** *(revision of S1-23xxxx)*

**Source: Deutsche Telekom AG, Nokia**

**pCR Title: Update of subclause security**

**Draft Spec: 3GPP TS 22.137 v.1.0.0**

**Agenda item: 7.1.2**

**Document for: Approval**

**Contact: Vasil Aleksiev, Vasil dot Aleksiev at magenta dot at**

*Abstract: This pCR proposes update of security functional service requirements*

**1. Introduction**

At 3GPP SA1#103 additional consolidated potential requirements were agreed and these need to be introduced into normative work.

**2. Reason for Change**

Adding of the agreed security CPRs from the FS\_Sensing study is needed to finalize normative work.

**4. Proposal**

It is proposed to agree the following changes to 3GPP TS 22.137 v.1.0.0.

\* \* \* First Change \* \* \* \*

### 5.2.4 Security

The 5G system shall support encryption, integrity protection, privacy of the 3GPP sensing data, non-3GPP sensing data and sensing results, to protect the data inside the 5G system.

The 5G system shall provide a mechanism to protect identifiable information that can be derived from the 3GPP sensing data from eavesdropping.

The 5G network shall limit the exposure of the sensing results only to a trusted third-party authorized to receive that sensing results.

The 5G system shall support appropriate sensing KPIs of 5G wireless sensing for both situations where consent can be obtained, and where it cannot.

Subject to regulation and user’s consent, the 5G network may associate sensing results and identity of the user together for further processing for a sensing target that has a UE and the UE is subscribed in the same network.

\* \* \* End of Changes \* \* \* \*