

EU DECLARATION OF CONFORMITY — BLETA TAB BT10-G4

EU DECLARATION OF CONFORMITY

Document reference: Bleta-DOC-BT10-G4-001 **Issue:** 1 **Issue date:** 22 May 2026

1. Product

Product: Portable tablet computer kit **Trade name:** Bleta Tab **Model:** BT10-G4 **Kit composition:** - Tablet hardware base: Lenovo TB311XU (Machine Types ZAEJ, ZAEL — LTE + WiFi variant) - Bleta Launcher software (custom Android launcher, pre-installed) - USB-C charger (Lenovo MC-202L, 20 W, USB Power Delivery) - USB-C cable - SIM ejector tool - Rotating tablet case (accessory) - Stylus pen with rubber-tip touch pointer (accessory)

Bleta Launcher software version: as installed at production; updates governed by section 7 below.

2. Manufacturer

Name: Bleta Solutions, S.L. **Address:** Av. Maresme 70 Bis, Nave 6, Planta 1, 08940 Cornellà de Llobregat, Barcelona, Spain **Tax identification (NIF/CIF):** B06961601 **VAT identification (EU):** ESB06961601 **Trade name:** BLETA (registered trademark) **Contact:** contact@bleta.io **Person responsible for compliance information under Article 4 of Regulation (EU) 2019/1020 (2019/1020):** Bleta Solutions, S.L. (the manufacturer above is the EU-established economic operator responsible for the tasks set out in Article 4(3) of that Regulation) — contact@bleta.io

This declaration of conformity is issued under the sole responsibility of the manufacturer.

3. Object of the declaration

The product identified in section 1 above. The product is placed on the EU market under the manufacturer's own brand pursuant to Blue Guide 2022 §2.3 and the manufacturer's own-brand rule of Regulation (EU) 2023/988 (2023/988), under which a person placing a product on the EU market under their own name or trademark is considered the manufacturer for purposes of that Regulation; Bleta Solutions, S.L. assumes the obligations of the manufacturer for the kit placed on the market.

The Bleta Launcher software layer modifies the Android user interface only. It does not alter the radio characteristics, firmware or kernel of the underlying device; the conformity of the radio and underlying operating system layers is supported by evidence from the original equipment supplier (Lenovo PC HK Limited).

4. Object of the declaration is in conformity with the relevant Union harmonisation legislation

Reference	Title
Directive 2014/53/EU (2014/53)	Radio Equipment Directive (RED)
Commission Delegated Regulation (EU) 2022/30 (2022/30)	Activating Article 3(3)(d), (e), (f) of Directive 2014/53/EU
Directive 2011/65/EU (2011/65) as amended by Commission Delegated Directive (EU) 2015/863 (2015/863)	Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment (RoHS)
Regulation (EU) 2023/1542 (2023/1542)	Batteries and Waste Batteries
Commission Regulation (EU) 2019/1782 (2019/1782)	Ecodesign of External Power Supplies
Directive (EU) 2022/2380 (2022/2380)	Common Charger Directive
Directive (EU) 2019/882 (2019/882)	European Accessibility Act (EAA)

The kit is also placed on the market in compliance with Regulation (EU) 2023/988 (2023/988) (General Product Safety Regulation); the internal risk assessment is documented in the technical file.

5. References to the relevant harmonised standards used

5.1 RED — Article 3.1(a) Health and Safety

- EN 50566:2017/A1:2023
- EN 62209-2:2010/A1:2019
- EN IEC 62368-1:2020+A11:2020
- EN 50332-1:2013
- EN 50332-2:2013

5.2 RED — Article 3.1(b) Electromagnetic Compatibility

- ETSI EN 301 489-1 V2.2.3 (2019-11)
- ETSI EN 301 489-3 V2.3.2 (2023-01)
- ETSI EN 301 489-17 V3.3.1 (2024-09)
- ETSI EN 301 489-19 V2.2.1 (2022-09)
- ETSI EN 301 489-52 V1.3.1 (2024-11)
- EN 55032:2015+A11:2020
- EN 55035:2017+A11:2020
- EN IEC 61000-3-2:2019+A1:2021
- EN IEC 61000-3-3:2013+A2:2021

5.3 RED — Article 3.2 Radio Spectrum

- EN 303 413 V1.2.1 (2021-04)
- EN 300 328 V2.2.2 (2019-07)
- EN 301 893 V2.1.1 (2017-05)
- EN 301 511 V12.5.1 (2017-03)
- EN 301 908-1 V15.2.1 (2023-01)
- EN 301 908-2 V13.1.1 (2020-06)
- EN 301 908-13 V13.3.1
- EN 300 440 V2.2.1 (2018-07)
- EN 303 345-1 V1.1.1 (2019-06)
- EN 303 345-3 V1.1.1 (2021-06)

5.4 RED — Article 3.3(d) Network Protection

- EN 18031-1:2024

EN 18031-1:2024 was published in OJEU by Commission Implementing Decision (EU) 2025/138 (2025/138) with a restriction stating that the standard does not confer presumption of conformity if, when applying its clauses 6.2.5.1 and 6.2.5.2, the user is allowed not to set and use any password. The conformity assessment route used for Article 3.3(d) on the Bleta Tab is **EU-type Examination (Module B) followed by Internal Production Control (Module C)** under Annex III of RED, on the basis of the EU-type Examination Certificate referenced in §6 below; presumption of conformity for the cybersecurity essential requirements derives from the Notified Body certificate independently of the OJEU restriction, which limits presumption under Module A (harmonised standard) only. On the substantive question addressed by clauses 6.2.5, the Bleta Tab as placed on the market preserves the screen-lock prompting mechanism of the underlying device as type-examined by the Notified Body: the Bleta Launcher's own onboarding flow does not include a password-configuration step, but the underlying Android system continues to surface, post-onboarding, a notification prompting the user to configure a screen lock, which leads the user to the Settings → Security & Privacy screen with an explicit set-up call-to-action for a PIN, pattern or password. The Notified Body's professional judgement, reflected in the issued certificate, treats the device's combined safeguards (encryption-at-rest enabled by default, screen-lock capability available via Settings, account management at OS level, and the post-onboarding screen-lock prompt of the underlying system) as satisfying the essential requirement of Article 3.3(d). EN 18031-1 is listed in this section as the technical reference applied in product design and gap analysis; the onboarding design rationale and the GPSR Article 7 (2023/988) risk-proportionality analysis are documented in the technical file.

5.5 RED — Article 3.3(e) Personal Data and Privacy Protection

- EN 18031-2:2024

EN 18031-2:2024 was published in OJEU by Commission Implementing Decision (EU) 2025/138 with the same password-setup restriction referenced in §5.4 above, plus an additional restriction stating that the standard does not confer presumption of conformity for equipment covered by its clauses 6.1.3–6.1.6 (childcare, toy, or wearable equipment) if parental or guardian access control is not ensured. The analysis of the password-setup restriction and the Module B / Module C conformity route apply equivalently to EN 18031-2. The additional childcare/toy/wearable restriction does not apply to the Bleta Tab, which is a general-purpose tablet placed on the market for an adult senior user target — not childcare, toy, or wearable equipment within the meaning of the standard.

5.6 RED — Article 3.4 Common Charger

- EN IEC 62680-1-2:2022
- EN IEC 62680-1-3:2022

5.7 RoHS Directive

- EN IEC 63000:2018

5.8 Ecodesign Directive

Conformity with Commission Regulation (EU) 2019/1782 has been demonstrated by application of the regulation directly to the external power supply.

5.9 European Accessibility Act

Conformity with the accessibility requirements of Annex I of Directive (EU) 2019/882 has been demonstrated by direct application of those requirements; design decisions documented in the technical file.

6. Notified Body involvement

Notified Body	NB Number	Scope of intervention	Certificate reference	Date of issue
KL-Certification GmbH	2784	EU-type Examination of the radio equipment under Article 3.2 (Radio Spectrum)	T.2024.10.0002 (TB311XU)	24 October 2024
SGS Fimko Oy	0598	EU-type Examination of the radio equipment under Article 3.3(d), (e), (f) (Cybersecurity)	RED-3500 Issue 2	18 July 2025

The conformity assessment procedure followed for the radio equipment is **Annex III of Directive 2014/53/EU (Module B + Module C)** for the articles covered by the EU-type Examination Certificates above, and **Annex II of Directive 2014/53/EU (Module A — Internal Production Control)** for the remaining requirements.

Note on Article 3.3(f) scope: the cybersecurity EU-type Examination Certificate listed above covers Article 3.3 letters (d), (e) **and (f)**. For the Bleta Tab as placed on the market, **Article 3.3(f) is not applicable:** the product does not enable money or virtual-money transfers within the scope set by Commission Delegated Regulation (EU) 2022/30 ([2022/30](#)) Article 3, which restricts (f) to “internet radio equipment which enables money or virtual money transfers”. Accordingly, no standard for Article 3.3(f) is cited in §5 above; the (f) coverage in the certificate’s scope is inherited from the underlying hardware certification and recorded here for completeness.

7. Additional information

7.1 Conformity of accessories

The kit includes accessories (rotating case, stylus pen) supplied by third parties. Their conformity with the General Product Safety Regulation (EU) 2023/988 ([2023/988](#)) and Regulation (EC) 1907/2006 ([1907/2006](#)) (REACH) is supported by supplier declarations archived in the manufacturer’s technical file.

7.2 Software updates and security support

The Bleta Tab follows a **managed update model** designed to preserve the stability of the senior-oriented user experience deployed via B2B channels. Security responses are delivered through one or more of the following channels, depending on the nature and severity of the issue:

- **Remote feature flags** (Firebase Remote Config / Realtime Database) for behavioural mitigation that does not require code changes.
- **Over-the-air updates** from the underlying device platform where enabled and operationally appropriate.
- **Exceptional code-level updates** pushed through the distribution channel (Lenovo Customization Service or equivalent), evaluated case-by-case for critical issues affecting the deployed fleet.
- **New product batches** placed on the market incorporate the latest software fixes.
- **Public advisories** issued where mitigation actions require end-user awareness.

Bleta Solutions, S.L. commits to providing security responses for this product for at least 5 years from the date this product is first placed on the EU market through the channels above. The scope of **code-level security updates** is inherited from the underlying Lenovo Tab hardware platform (TB311XU) and is expected to extend through Q4 2028 per Lenovo’s published support commitment; the corresponding declaration is published at <https://bleta.io/compliance>. The vulnerability handling process is documented in the technical file. Vulnerability reports may be submitted to security@bleta.io; see also <https://bleta.io/well-known/security.txt>.

7.3 Technical file location

The technical documentation supporting this declaration is maintained at the registered office of the manufacturer and is available to market surveillance authorities upon request, for at least 10 years from the date the last unit was placed on the market.

7.4 Where to obtain this declaration

The full EU Declaration of Conformity is published at: <https://bleta.io/conformity/bleta-tab>.

8. Signed for and on behalf of Bleta Solutions, S.L.

Place of issue: Barcelona, Spain **Date of issue:** 22 May 2026

Name: Isabel García Baños **Function:** Sole Director (Administradora única)

Signature:

Isabel García Baños Bleta Solutions, S.L.