EU DECLARATION OF CONFORMITY

[MANUFACTURER LETTERHEAD] *Insert company logo, name, address, and contact details here*

DoC Reference Number: [INSERT INTERNAL REFERENCE No.]

1. MANUFACTURER

The manufacturer details must be set out as follows:

Field	Details
Company Name	[Full Legal Name of Manufacturer]
Registered Address	[Street, City, Postal Code, Country]
Contact (Email / Tel)	[manufacturer@example.com / +XX XXX XXX XXXX]

2. AUTHORIZED REPRESENTATIVE IN THE EU *(if applicable)*

This section is required where the manufacturer is established outside the European Union. If not applicable, delete this section.

Field	Details
Company Name	[Full Legal Name of EU Authorized Representative]
Registered Address	[Street, City, Postal Code, EU Member State]
Contact (Email / Tel)	[rep@example.com / +XX XXX XXX XXXX]

2A. RESPONSIBLE ECONOMIC OPERATOR IN THE EU — Article 4, Regulation (EU) 2019/1020 *(non-EU manufacturers only)*

When to use this section: Regulation (EU) 2019/1020, in force since 16 July 2021, mandates that all businesses outside the EU selling certain products directly or indirectly — including through e-commerce platforms — must have an economic operator within the EU. This economic operator acts as a liaison between the non-EU manufacturer and EU Market Surveillance Authorities (MSA), ensuring product compliance and consumer safety. That economic operator may be the same entity as the Authorized Representative in Section 2, or it may be a different party — for example, an importer or a fulfilment service provider. Where they are the same, cross-reference Section 2 and note "same as Section 2." Where they differ, complete this section separately.

The economic operator's name and address must be clearly visible on the product or its packaging.

If the manufacturer is established within the EU, delete this section entirely.

Field	Details
Role of Responsible Economic Operator	[Authorized Representative / Importer / Fulfilment Service Provider — select as applicable]
Company Name	[Full Legal Name]
Registered Address (EU)	[Street, City, Postal Code, EU Member State]
Contact (Email / Tel)	[contact@example.com / +XX XXX XXX XXXX]
Basis of Responsibility	[Article 4(1) of Regulation (EU) 2019/1020 — economic operator responsible for product compliance and liaison with EU Market Surveillance Authorities]

Same as Section 2?	[Yes — same entity / No — separate entity as identified above]

Note on fulfilment service providers: Fulfilment service providers, such as Amazon, are considered economic operators under this regulation and are responsible for verifying and maintaining the technical file and Declaration of Conformity, unless these responsibilities are transferred to another economic operator within the EU. Where such responsibilities are transferred to an Authorized Representative or importer, that transfer should be documented and the responsible entity identified in this section.

3. PRODUCT IDENTIFICATION

Annex III of Decision 768/2008/EC requires identification sufficient to allow traceability between the Declaration and a specific unit or production run. A photograph of the product may be attached where text alone is insufficient.

Field	Details
Product Name / Description	[e.g., "Wireless Bluetooth Speaker"]
Product Model / Type	[e.g., Model XYZ-100]
Batch / Serial Number(s)	[e.g., Batch No. 2024-001, or Serial No. range XXXXXXXX–XXXXXXXX]
Intended Use	[e.g., Consumer electronic device for audio playback via Bluetooth]
Country of Origin	[e.g., China / Germany]
Hardware Version *(CRA — where applicable)*	[e.g., Rev C / PCB v3.2]
Software / Firmware Version *(CRA — where applicable)*	[e.g., v2.4.1 — insert version number at time of this Declaration]

The hardware version and software/firmware version fields are required under the Cyber Resilience Act (Regulation (EU) 2024/2847) for products with digital elements. They may be omitted for products that have no digital elements and to which the CRA does not apply.

4. DECLARATION OF SOLE RESPONSIBILITY

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

Note for CRA-scoped products: The Cyber Resilience Act uses the term **"provider"** rather than "manufacturer" for conformity responsibility purposes. Where the CRA applies to this product, the above statement should be read as: *"This declaration of conformity is issued under the sole responsibility of the provider."* Both formulations are acceptable within a single combined declaration covering multiple acts; however, where precision is required, manufacturers of products with digital elements may prefer to state both: *"This declaration of conformity is issued under the sole responsibility of the manufacturer/provider."*

5. APPLICABLE EU DIRECTIVES AND REGULATIONS

The manufacturer/provider hereby declares that the product described above is in conformity with the relevant Union harmonization legislation, as listed below:

Directive / Regulation	Reference	Official Journal
Low Voltage Directive *(see note below on RED relationship — delete if RED applies or if product is outside LVD voltage scope)*	Directive 2014/35/EU	OJ L 96, 29.3.2014

Electromagnetic Compatibility (EMC) Directive	Directive 2014/30/EU	OJ L 96, 29.3.2014
Radio Equipment Directive (RED) *(delete if not radio equipment; see note below on LVD relationship)*	Directive 2014/53/EU	OJ L 153, 22.5.2014
Restriction of Hazardous Substances (RoHS) Directive	Directive 2011/65/EU, as amended by Directive (EU) 2015/863	OJ L 174, 1.7.2011
Waste Electrical and Electronic Equipment (WEEE) Directive *(where applicable — typically evidenced by producer registration; verify applicability)*	Directive 2012/19/EU	OJ L 197, 24.7.2012
Cyber Resilience Act (CRA) *(applicable to products with digital elements — delete if product has no connectivity or software components; full DoC/CE-marking obligations mandatory for products placed on the EU market on or after 11 December 2027)*	Regulation (EU) 2024/2847	OJ L, 2024/2847, 20.11.2024

Note on the RED / LVD Relationship (Directive 2014/53/EU and Directive 2014/35/EU):

Where the Radio Equipment Directive applies to this product, the following interaction with the Low Voltage Directive must be understood:

- Under the Radio Equipment Directive (2014/53/EU), all radio equipment must comply with EMC and LVD requirements. Specifically, RED Article 3.1(a) requires that radio equipment be constructed to protect the health and safety of persons and domestic animals and the protection of property — covering the same safety objectives as the LVD.
- Critically, as per RED, there is **no voltage limit**. This means even battery-operated equipment must comply with the safety requirements. This is a fundamental distinction from the standalone LVD, which applies only to equipment designed for use with a voltage rating of between 50–1,000 V AC or 75–1,500 V DC: the LVD's lower voltage threshold does **not** apply under RED.
- As a result, where RED applies to a product, the safety objectives of LVD are effectively subsumed within RED Article 3.1(a), and it is **not necessary — and generally incorrect** — to list the standalone LVD as a separately applicable directive for that product. The LVD row in the table above should be deleted for all products within RED's scope.
- Harmonized safety standards (such as EN IEC 62368-1) applied to demonstrate compliance with RED Article 3.1(a) serve simultaneously as the basis for satisfying the safety essential requirement — without the manufacturer separately referencing LVD.

Manufacturers should verify their specific product scope and seek technical advice where the RED/LVD boundary is unclear.

Note on RED (Directive 2014/53/EU) additional mandatory content per Annex VI:

Where the product contains a radio transmitter/receiver, the following must also be stated in this Declaration:

- **Frequency band(s) of operation:** [e.g., 2.400–2.4835 GHz (Bluetooth/Wi-Fi); 5.150–5.850 GHz (Wi-Fi 5 GHz)]
- **Maximum radio-frequency power transmitted:** [e.g., ≤ 20 dBm EIRP]
- **Cybersecurity requirements** (where applicable under Commission Delegated Regulation (EU) 2022/30): [Confirm compliance or state "Not applicable" — note: from 11 December 2027, the CRA row above will supersede and replace this sub-requirement for most digital products]

Note on CRA (Regulation (EU) 2024/2847):

The Cyber Resilience Act (Regulation (EU) 2024/2847) is the EU's first product cybersecurity law, requiring manufacturers and distributors of hardware and software with digital elements to embed

security throughout the product lifecycle. It is in force since December 10, 2024, with full compliance required by December 11, 2027.

CRA mandates vulnerability management (5-year support), SBOM documentation, ENISA incident reporting within 24 hours, and CE marking for digital products — with penalties up to €15 million or 2.5% of global annual turnover.

Where the CRA applies, the additional CRA-specific information required is set out in Section 5A below.

5A. CRA SUPPLEMENTARY INFORMATION *(Cyber Resilience Act — delete if CRA does not apply)*

CRA applies to any manufacturer, importer, or distributor that places a "product with digital elements" on the EU market, regardless of where they are headquartered.

Field	Details
Product Classification under CRA	[Default class (self-declaration) / Important — Category I (Annex III) / Critical — Category II (Annex IV)]
Conformity Assessment Route (CRA)	[Self-declaration — Module A (default class) / Third-party assessment by Notified Body (Category I or II) / European Cybersecurity Certificate at "substantial" level (Category I) / European Cybersecurity Certificate at "high" level (Category II)]
Cybersecurity Risk Assessment Conducted	[Yes — retained in technical file dated DD/MM/YYYY]
Security-by-Design Compliance	[Confirmed — product ships with no known exploitable vulnerabilities, secure-by-default configuration, encrypted communications, minimized attack surface, and least privilege per Annex I, Part I, point (2) of Regulation (EU) 2024/2847]
SBOM Prepared and Maintained	[Yes — Software Bill of Materials prepared in [CycloneDX / SPDX] machine-readable format per Annex I, Part II, point (1); maintained and available to Market Surveillance Authorities upon request]
Coordinated Vulnerability Disclosure (CVD) Policy	[Published at: https://[company.com]/.well-known/security.txt / [security@company.com]]
Vulnerability Reporting to ENISA	[Manufacturer commits to reporting actively exploited vulnerabilities to ENISA within 24 hours per Article 14 of Regulation (EU) 2024/2847, effective 11 September 2026]
Support Period	[Security updates provided until DD/MM/YYYY — minimum 5 years from first EU market placement, per Article 13(8), unless expected in-use period is shorter]
First EU Market Placement	[DD/MM/YYYY]
CRA Notified Body *(Category I / II only — delete for default-class products)*	[Full Name of CRA Notified Body / NANDO Number / Certificate Reference]

6. HARMONIZED STANDARDS AND TECHNICAL SPECIFICATIONS APPLIED

The object of the declaration described above is in conformity with the relevant Union harmonization legislation. Conformity is based on the following harmonized European standards (dated editions as published in the Official Journal of the EU):

6.1 Low Voltage Directive (LVD) — 2014/35/EU *(delete this subsection if RED applies — see Section 5 note)*

Reminder: As per RED, there is no voltage limit — even battery-operated equipment must comply with the safety requirements under RED Article 3.1(a). Where RED applies to this product, safety objectives are covered under Section 6.3 (RED standards) and this LVD sub-section should be deleted. The standards cited in 6.1 remain relevant only for products within LVD scope that are **not** also subject to RED.

Standard	Title	Dated Edition
[e.g., EN IEC 62368-1]	[Audio/video, information and communication technology equipment — Part 1: Safety requirements]	[e.g., :2020+A11:2020]
[EN XXXXX]	[Insert applicable harmonized standard]	[YYYY]

6.2 EMC Directive — 2014/30/EU

Standard	Title	Dated Edition
[e.g., EN 55032]	[Electromagnetic compatibility of multimedia equipment — Emission requirements]	[e.g., :2015+A2:2020]
[e.g., EN 55035]	[Electromagnetic compatibility of multimedia equipment — Immunity requirements]	[e.g., :2017+A11:2020]
[e.g., EN IEC 61000-3-2]	[Electromagnetic compatibility — Limits for harmonic current emissions]	[e.g., :2019+A1:2021]
[e.g., EN IEC 61000-3-3]	[Electromagnetic compatibility — Limitation of voltage changes, voltage fluctuations and flicker]	[e.g., :2013+A1:2019+A2:2021]

6.3 Radio Equipment Directive (RED) — 2014/53/EU *(delete if not applicable)*

Note: Standards applied under 6.3 include both the radio and safety requirements. Where a product contains a radio device, the whole product must show compliance with the relevant electrical safety standard — and there is no exemption based upon power for battery-operated devices. Safety standards listed here (such as EN IEC 62368-1) therefore serve to demonstrate conformity with RED Article 3.1(a) and the standalone LVD section (6.1) should be deleted.

Standard	Title	Dated Edition
[e.g., EN IEC 62368-1]	[Audio/video, information and communication technology equipment — Part 1: Safety requirements — applied pursuant to RED Art. 3.1(a)]	[e.g., :2020+A11:2020]
[e.g., EN 301 489-1]	[EMC standard for radio equipment — Part 1: Common technical requirements]	[e.g., V2.2.3 (2019-11)]
[e.g., EN 301 489-17]	[EMC standard — Specific conditions for Broadband Data Transmission Systems]	[e.g., V3.2.4 (2020-09)]
[e.g., EN 300 328]	[Wideband transmission systems — Data transmission equipment operating in the 2,4 GHz ISM band]	[e.g., V2.2.2 (2019-07)]
[e.g., EN IEC 62311]	[Assessment of electronic and electrical equipment related to human exposure restrictions for electromagnetic fields]	[e.g., :2020]

6.4 RoHS Directive — 2011/65/EU

Standard	Title	Dated Edition
[e.g., EN IEC 63000]	[Technical documentation for the assessment of electrical and electronic products with respect to the restriction of hazardous substances]	[e.g., :2018]

The WEEE Directive does not mandate a separate conformity standard but requires producer registration with national WEEE registries and proper product marking (crossed-out wheelie bin symbol).

WEEE Producer Registration Number: [Insert national WEEE registry registration number(s)]

6.5 Cyber Resilience Act (CRA) — Regulation (EU) 2024/2847 *(delete if not applicable)*

The CRA's binding SBOM mandate sits in Annex I, Part II, point (1): manufacturers must identify and document the components in their products, including by drawing up a software bill of materials in a commonly used, machine-readable format covering at least the top-level dependencies.

At the time of this Declaration, no harmonized European standards have been formally published in the Official Journal of the EU specifically under the CRA. Where such standards are published, this section should be updated. In the interim, manufacturers must demonstrate conformity directly against the essential requirements of Annex I of Regulation (EU) 2024/2847 and may reference relevant technical specifications or available standards as guidance.

Standard / Specification	Title	Dated Edition / Status
[e.g., EN 18031 series]	[Cybersecurity requirements for connected products — CRA harmonized standard series, in development by ETSI/CEN-CENELEC]	[Insert dated edition when published in OJ — pending as at date of this Declaration]
[e.g., ETSI EN 303 645]	[ETSI Cyber Security for Consumer Internet of Things: Baseline Requirements — applied as guidance pending CRA harmonized standards]	[e.g., V2.1.1 (2020-06)]
[e.g., ISO/IEC 27001]	[Information security management — applied as a complementary reference for organisational controls]	[e.g., :2022]
[EN XXXXX — insert when published]	[CRA harmonized standard — insert title and edition upon publication in OJ]	[YYYY]

Where no harmonized CRA standard has been applied, manufacturers must state the alternative technical basis for conformity, for example: "Conformity with the essential cybersecurity requirements of Annex I of Regulation (EU) 2024/2847 is demonstrated by [describe approach, e.g., internal risk assessment per Article 13, SBOM compiled in CycloneDX/SPDX format, penetration testing conducted by [test body] on [date], secure development lifecycle procedures documented in the technical file]."

7. NOTIFIED BODY *(if applicable)*

A Notified Body is only involved where a conformity assessment module other than Module A applies (e.g., Module B, C2, H). Most standard consumer electronics rely on Module A (manufacturer's internal production control), in which case this section should be deleted. Do not name a Notified Body where no third-party assessment was performed.

CRA note: For important class products (Category I, Annex III), the manufacturer may either demonstrate conformity with a harmonized standard or engage a CRA-notified body for a full conformity assessment. For critical class products (Category II, Annex IV), a mandatory European Cybersecurity Certificate at "high" assurance level or a full notified body audit is required — self-

assessment is not permitted. Where a CRA Notified Body has been engaged, complete the table below separately for CRA (in addition to any Notified Body engaged under LVD/RED).

Field	Details
Notified Body Name	[Full Name of Notified Body]
Notified Body Number (NANDO)	[4-digit EU Notified Body ID, e.g., XXXX]
Directive / Regulation	[e.g., RED — Directive 2014/53/EU / CRA — Regulation (EU) 2024/2847]
Conformity Assessment Procedure	[e.g., Module B — EU type-examination / Module C2 — Conformity to type / CRA third-party assessment per Article 32]
Certificate Number	[e.g., Certificate No. XXXX-YYYY-ZZZZ]
Certificate Date	[DD/MM/YYYY]

8. ADDITIONAL INFORMATION

Field	Details
Technical File Location	[Name and address of person/entity in the EU responsible for the technical file, where different from the manufacturer]
Technical File Custodian	[Name, Title, Address]
SBOM Location / Availability *(CRA — where applicable)*	[SBOM available to Market Surveillance Authorities upon request from: [contact/address]; format: CycloneDX / SPDX; version: [X.X]; last updated: DD/MM/YYYY]
Cybersecurity Risk Assessment Reference *(CRA — where applicable)*	[Risk assessment document reference; date; retained in technical file at [location]]
Supplementary Remarks	[Any additional information required by sector-specific acts or applicable national legislation]

9. CONFORMITY STATEMENT

The object of the declaration described above is in conformity with the relevant Union harmonization legislation.

This Declaration of Conformity entitles the product to bear the CE marking. The CE marking must not be affixed until all obligations under the applicable directives and regulations have been fulfilled and this Declaration has been properly signed.

CE Marking Affixed: ☐ Yes — as of [DD/MM/YYYY]

Note on the CE marking affixing date field: This field is retained for internal record-keeping and quality management purposes. It is not strictly required as a mandatory element of a Declaration of Conformity under modern EU harmonization legislation. The **Date of Issue** in Section 10 below constitutes the legally operative date of the Declaration and suffices for regulatory purposes. The CE marking affixing date in this section may be retained, omitted, or moved to the technical file at the manufacturer's discretion; however, where it is completed, it must be accurate — the CE marking must not be affixed prior to the completion of all conformity obligations and the proper signing of this Declaration.

10. PLACE AND DATE OF ISSUE

Field	Details

Place of Issue	[City, Country]
Date of Issue	[DD/MM/YYYY]

11. SIGNATURE BLOCK

Field	Details
Signed for and on behalf of	[Full Legal Name of Manufacturer / Provider / Authorized Representative]
Name of Signatory	[First Name Last Name]
Position / Function	[e.g., Chief Technical Officer / Head of Regulatory Affairs]
Signature	_____
Date	[DD/MM/YYYY]

This Declaration of Conformity must be retained for a minimum of 10 years from the date on which the last unit of this product model is placed on the EU market, in accordance with the applicable directives, and made available to Market Surveillance Authorities upon request. Where the CRA applies and the product's support period exceeds 10 years, the Declaration — together with the SBOM and technical file — must be retained for the full duration of that support period.

DRAFTING NOTES FOR MANUFACTURERS

The following notes are for internal use and should be removed before the DoC is finalized and signed.

1. **Single Declaration, Multiple Acts.** A product covered by the Low Voltage Directive, EMC Directive, RoHS Directive, and Radio Equipment Directive requires one Declaration of Conformity listing all applicable acts. The single-document approach is the Commission's preferred form (Blue Guide 2022, §4.4). The CRA is added to this single declaration in the same way.
2. **Dated Standard Editions Are Mandatory.** Citing harmonized standards by year only, without a dated edition, is a common error. "EN 60204-1" is ambiguous; "EN 60204-1:2018" identifies the dated edition. Each act requires the dated edition published in the Official Journal of the EU.
3. **Do Not List Inapplicable Directives.** Adding the Low Voltage Directive to the DoC of a product not within LVD's voltage range is a substantive error. The DoC declares conformity with every act listed; listing an inapplicable act creates a false declaration. Equally, listing the CRA for a product with no digital elements and no connectivity is an error.
4. **RED replaces LVD for radio products.** As per RED, there is no voltage limit — even battery-operated equipment must comply with the safety requirements. Delete the standalone LVD row and Section 6.1 for any product within RED's scope. Apply safety standards in Section 6.3 instead, clearly noting they are applied pursuant to RED Article 3.1(a).
5. **Article 4 of Regulation (EU) 2019/1020 — Responsible Economic Operator.** Regulation (EU) 2019/1020 mandates that all businesses outside the EU selling certain products must have an economic operator within the EU. Section 2A has been added to capture this requirement. The responsible economic operator may be the same entity as the Authorized Representative or a different entity such as an importer. Both their name and address must be on the product or packaging.
6. **CRA Timing.** The CRA is in force since December 10, 2024, with full compliance required by December 11, 2027. Article 14 reporting of actively exploited vulnerabilities starts 11 September 2026. Manufacturers should not wait until 2027 to begin SBOM preparation and vulnerability disclosure policy implementation — both take significant lead time.
7. **CRA SBOM Obligation.** Annex I, Part II, point (1) requires manufacturers to identify and document the components in their products, including by drawing up a software bill of materials in a commonly used, machine-readable format covering at least the top-level

dependencies — and to keep it up to date for the support period. The CRA does not mandate a specific standard, so use CycloneDX or SPDX, both of which market surveillance authorities recognize.

8. **CRA Vulnerability Handling.** Manufacturers must notify ENISA (the EU Cybersecurity Agency) within 24 hours of becoming aware that a vulnerability in their product is being actively exploited. A fuller notification must follow within 72 hours, and a final report within 14 days once a corrective measure is available. This reporting channel is separate from, but may overlap with, NIS2 obligations.
9. **CRA Conformity Assessment Route.** Most products can self-declare CRA conformity by completing an internal risk assessment, ensuring all requirements are met, and affixing the CE mark. Important class (Category I) products require third-party assessment or application of harmonized standards; critical class (Category II) products require a European Cybersecurity Certificate at "high" level or a full notified body audit. Confirm classification against Annexes III and IV of the CRA before selecting a conformity route.
10. **Notified Body for Module A / CRA default class.** No Notified Body is involved in Module A. Similarly, no Notified Body is required for CRA default-class products. Listing one creates a false record of a conformity assessment that did not occur.
11. **Language Requirements.** The Declaration must be translated into the language(s) required by the Member State in which the product is placed on the market or made available. In practice, manufacturers provide the Declaration in English plus the language of each Member State of destination.
12. **Retention Period.** The Declaration is part of the technical file and must be retained for 10 years from the last unit placed on the market for most acts. Under the CRA, if the support period exceeds 10 years, the retention period extends to match it. The SBOM must equally be retained for this full period.
13. **RED Simplified Declaration.** Under Article 18(2) of the Radio Equipment Directive 2014/53/EU, a simplified Declaration may be supplied via an internet address printed on the product or its packaging, provided the full Declaration is available at that address.
14. **Consequences of a False or Missing Declaration.** An incorrect or missing Declaration is a formal non-compliance in its own right. Under Article 16 of Regulation (EU) 2019/1020, a market surveillance authority finding a missing or non-compliant Declaration may require the economic operator to bring the product into conformity, withdraw it, or recall it. Under the CRA, non-compliance with essential cybersecurity requirements can trigger fines of up to €15 million or 2.5% of global annual turnover.

Sources: Decision No 768/2008/EC, Annex III; Directive 2014/35/EU (LVD); Directive 2014/30/EU (EMC); Directive 2014/53/EU (RED); Directive 2011/65/EU (RoHS); Directive 2012/19/EU (WEEE); Regulation (EU) 2024/2847 (CRA — OJ L, 2024/2847, 20.11.2024); Regulation (EU) 2019/1020 (Market Surveillance Regulation, in force 16 July 2021); Commission Notice — Blue Guide 2022, §4.4 (EUR-Lex); EMC Tech — RED Directive and LVD interaction (emctech.com.au); 24hour-AR — Understanding Regulation (EU) 2019/1020 (24hour-ar.com); EuroComply — CRA Compliance Guide (eurocomply.app); O3 Security — EU CRA SBOM and Vulnerability Requirements (o3.security).