INTRODUCING

CYBERSECURITY RISK ASSESSMENT

The CRA Cornerstone

CYBER RESILIENCE ACT: BUILDING A CYBERSECURE FUTURE

05/05/2025

Maria Raphael

ABOUT US

BACKGROUND

Founded in Larnaka, Cyprus, Raphael Legal and Privacy Minders provide comprehensive legal services designed to meet the evolving needs of businesses in today's complex legal environment. Our experienced team of legal experts specializes in global legal consultancy and compliance services, covering a wide range of areas including corporate law, business administration, financial services, tax law, trust law, shipping and maritime law, data protection, technology, digital information, and digital law regulatory frameworks.

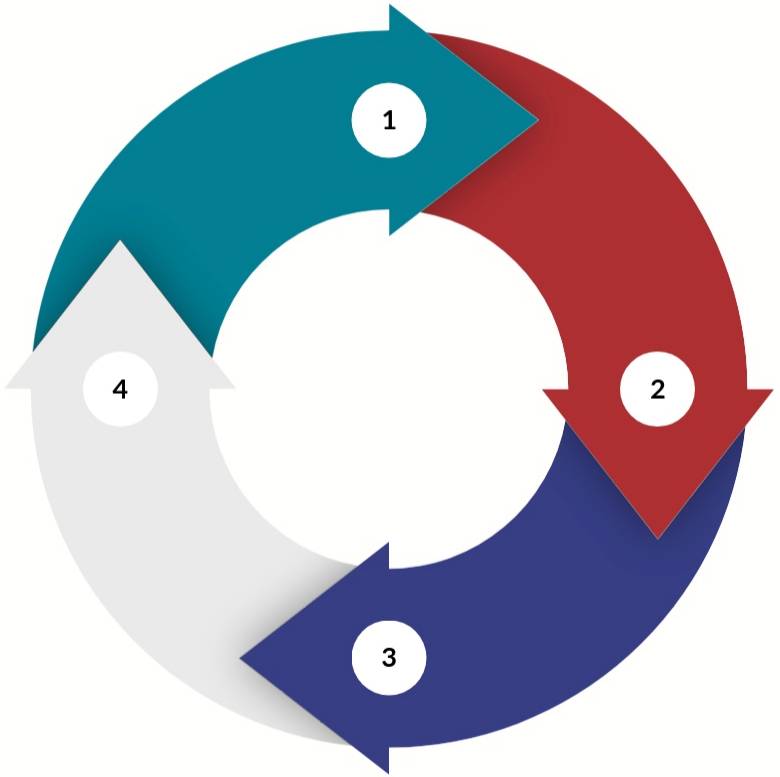
Raphael Legal

OUR MISSION

At Raphael Legal and Privacy Minders, we follow a holistic approach, offering a full range of legal and compliance protection services with extensive international reach and a client-centric focus approach.

Our aim is to provide the highest standard of services through strategic thinking and implementation. This ensures the protection of our clients' operational, reputational, and legal business objectives and interests.

MAKING AVAILABLE ON THE MARKET CONDITIONS



1. **Annex I, Part 1 (1) CRA**: Design, Development and Production of PDE in a way that they ensure an appropriate level of cybersecurity based on the risks

2. **Annex I, Part 1 (2) CRA**: Cybersecurity Controls

3. **Conditions for meeting (1) and (2)**: Properly Installed, used for their intended purpose or under conditions which can reasonably be foreseen, and, where applicable, the necessary security updates have been installed.

4. **Annex I, Part 2 CRA**: Vulnerability Handling Requirements

CRA ESSENTIAL CYBERSECURITY REQUIREMENTS ANNEX I, PART 1 (2)

ON THE BASIS OF THE CYBERSECURITY RISK ASSESSMENT (art. 13 (2) of the CRA and, where applicable, PDE shall:

Vulnerability Handling
SR 15

1.PLANNING
2. DESIGN
3. DEVELOPMENT
4.PRODUCTION
5. DELIVERY
6. MAINTENANCE

- No Known exploitable vulnerabilities
- Secure by Default Configeneration
- Security Updates to address vulnerabilities
- Protection from unauthorized access
- Confidentiality Protection
- Integrity Protection
- Data Minimization
- Availability & Resilience of essential functions
- Minimize product or device impact on service availability.
- Attack surface reductions
- Incident impact mitigation
- Security Monitoring & Logging
- Permanent & Easy deletion of data and secure transfer of data

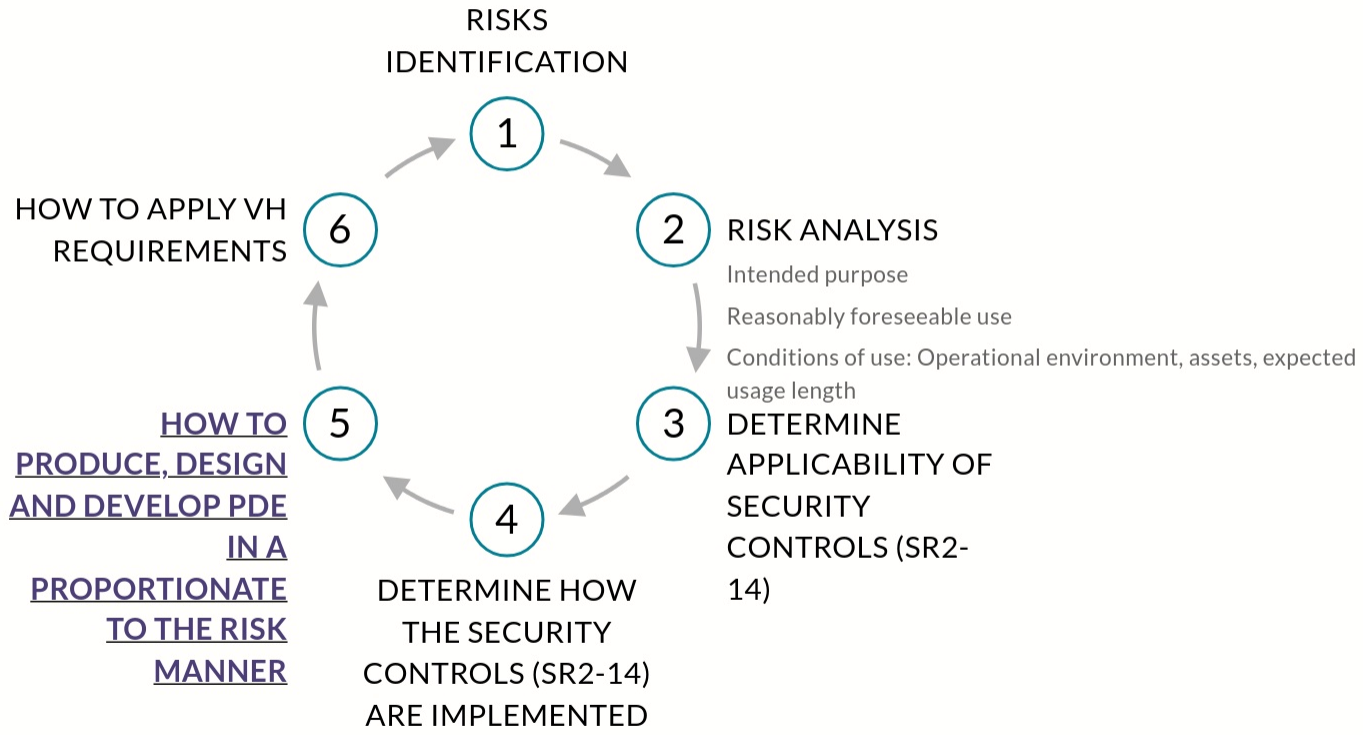
SR 2-14

RISK ASSESSMENT PROCESS (CONTINUOUS&SYSTEMATICALLY UPDATED): ART.13

OBJECTIVES

Minimize Risks

Prevent incidents and minimize their impact, including in relation to the health and safety of users

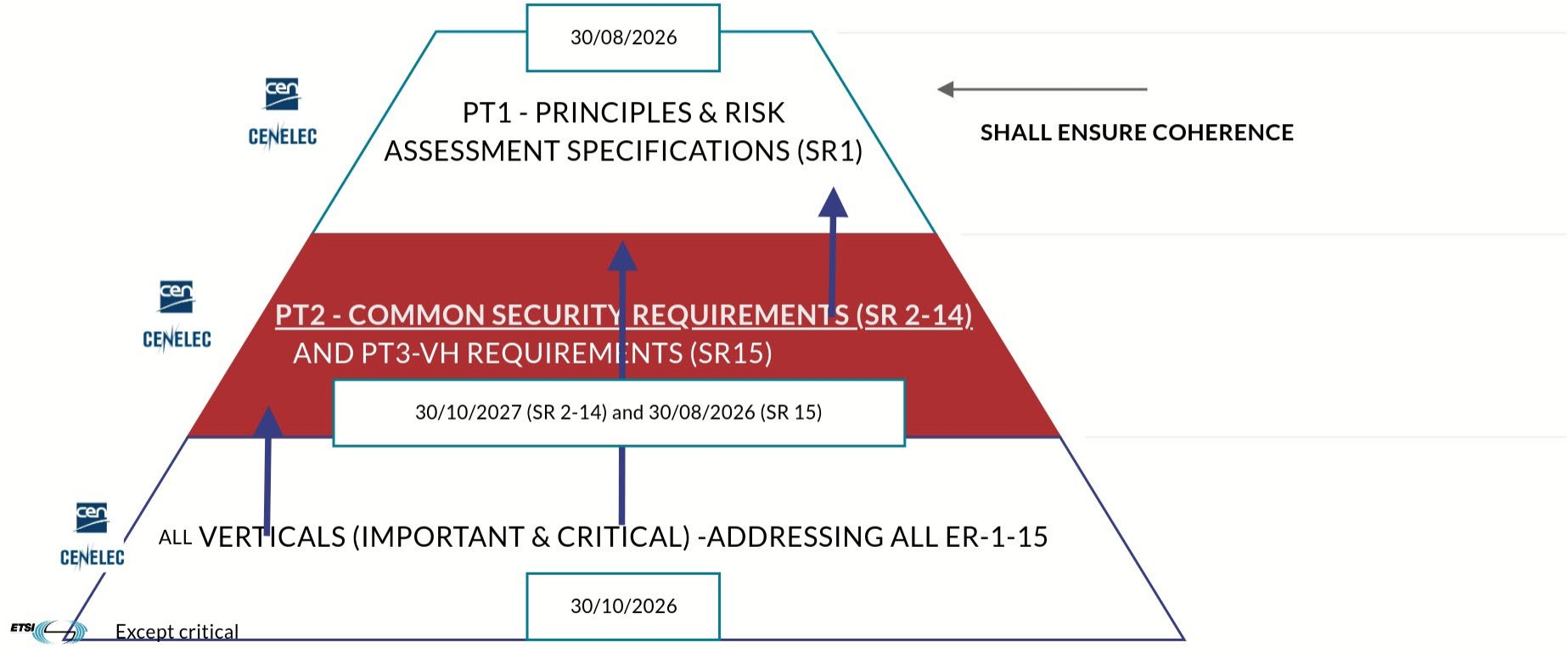


Includes due diligence for third-party components

Raphael Legal

PRIVACY MINDERS

PT1 STANDARD (PRINCIPLES & TECHNICAL SPEF. ON RISK ASSESSMENT)



THE SR THREATS DISCLOSURE & SUPPORTING REQUIREMENT

- **The Standards must clarify the threats covered, policies and assumptions.**
- The Standards shall support manufacturers in **identifying and specifying the threats, policies and assumptions:** This means that the manufacturers shall identify the threats that apply to them.
- Each harmonised European standard shall clearly .....**which risks are covered**, and **which other relevant risks are not covered.**

THE IDENTIFICATION OF CYBERSECURITY RISKS IS NOT LIMITED TO THOSE THAT MAP DIRECTLY TO THE ESSENTIAL REQUIREMENTS (ERS).

INSTEAD, THE RISK ASSESSMENT MUST BE CARRIED OUT FIRST TO IDENTIFY THE FULL SPECTRUM OF RISKS ASSOCIATED WITH THE PRODUCT.

BASED ON THIS ASSESSMENT, MANUFACTURERS DETERMINE WHICH ERS ARE APPLICABLE AND HOW THEY ARE TO BE IMPLEMENTED.

ER1 SERVES AS A RESIDUAL REQUIREMENT, ENSURING THAT ANY RISKS NOT SPECIFICALLY ADDRESSED BY ERS 2–15 ARE STILL COVERED.

AS A RESULT, SECURITY CONTROLS BEYOND THOSE LISTED IN ANNEX I, PART I (2) MAY BE REQUIRED TO APPROPRIATELY TREAT RESIDUAL RISKS.

THE ER1 REQUIREMENT

ALL PRODUCTS WITH DIGITAL ELEMENTS -DEFAULT (THAT DO NOT FALL UNDER ANNEX III, CLASS I AND CLASS II)

MODULE A
Self Declaration of Conformity
(No Harmonized Standards or Common Specifications or Scheme needed)

OPTIONALLY
All conformity Assessment Procedures: Modules B/C, H or Scheme

IMPORTANT PRODUCTS: ANNEX III, CLASS I

MODULE A & HARMONIZED STANDARDS

COMMON SPECIFICATIONS

CSA SCHEME
At least substantial

1 **MODULES B (EU Type Examination) AND C (Conformity to Type based on Internal Production Control)**

2 **MODULE H (Full quality Assurance)**

IMPORTANT PRODUCTS: ANNEX III, CLASS II

MODULES B AND C

MODULE H

CSA SCHEME (at least substantial)

ANNEX IIIA CRITICAL PRODUCTS (NOW ANNEX IV)

MANDATORY CSA SCHEME

MODULES B AND C (if Scheme X)

MODULE H (If Scheme X)

RISK ASSESSMENTS

MANUFACTURER'S RISK ASSESSMENT

Article 13 and Annex I, Part 1

Performs a risk analysis on specific products

Informs security by design, the application of cybersecurity requirements and vulnerability handling requirements throughout the product's lifecycle

It cannot declassify a product from the Critical, Important I or Important II category if it has the core functionality of such category

EC RISK ASSESSMENT

CRA Legislative Process

Classifies product categories (Important I and II and Critical)

Does the specific product fits the CORE FUNCTIONALITY of the category?

Informs the Conformity Assessment Path

The product categories may be updated by the European Commission

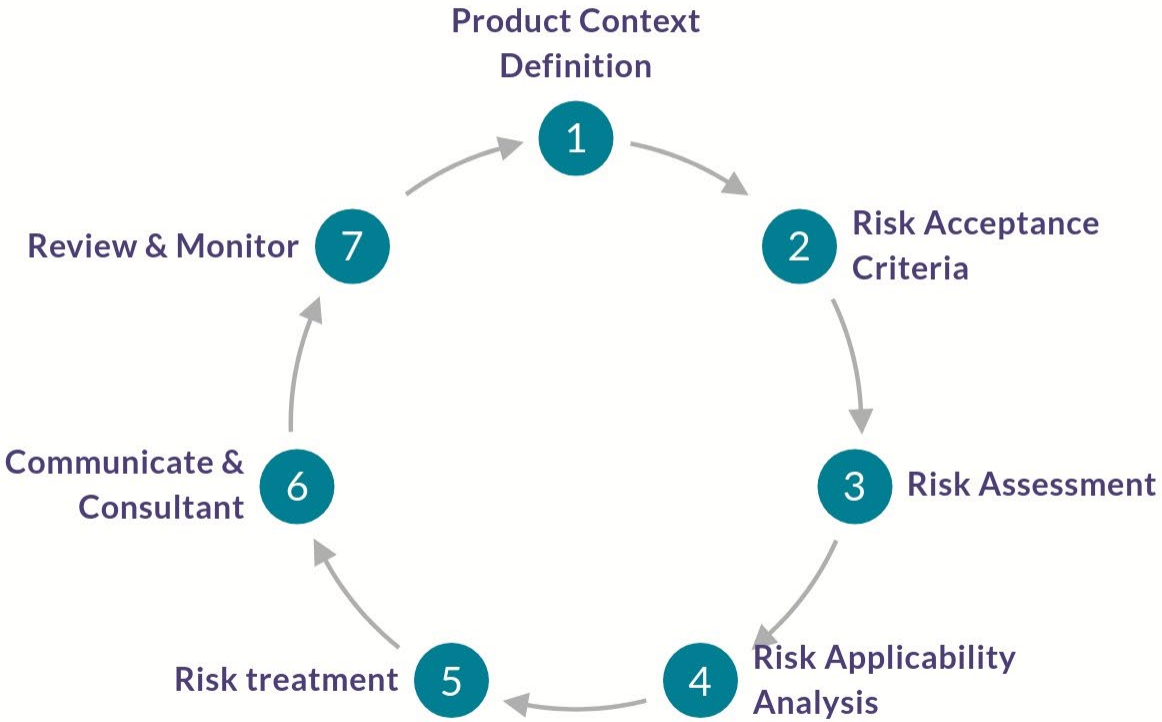
CORE FUNCTIONALITY

ELEMENTS	RISK ASSESSMENT	EXPLANATION	CORE FUNCTIONALITY	RELATIONSHIP TO CORE FUNCTIONALITY
Intended Purpose	✓	Explicit	✓	Explicit (fundamental features and capabilities)
Reasonably Foreseeable Use	✓	Explicit	✓	Explicit (fundamental features and capabilities)
Essential features/capabilities	⊗	Explicit	✓	Explicit
Fundamental functionalities /capabilities	✓	Subset of essential features, user triggered or continuously used (intended purpose)	✓	If they fulfil the primary purpose of the product (fundamental features and capabilities) and without it,. intented purpose or reasonably fopreseeable cannot be met
Product's user	✓	Reasonably Foreseeable Use	⊗	Reasonably Foreseeable Use
Operational Environment	✓	Explicit: Condition of use	⊗	Reasonably Foreseeable Use
Reasonably Foreseeable misuse	✓	Condition of use	⊗	Not relevant. Helps identify boundaries of intended purpose and reasonably foreseeable use.
Assets	✓	Explicit:Condition of use (Data and functions)	⊗	Only those assets that are indispensable for the product to achieve its primary purpose (fundamental features and capabilities)
System Architecture	✓	To analyse intended purpose, conditions of use, operational environment, assets	✗	
Lengh of time	✓	Explicit	✗	

Analyses risks

Classifies product

CYBERSECURITY RISK MANAGEMENT: PT1/WG9/JTC13



DUE DILIGENCE-THIRD PARTY COMPONENTS: PART OF RISK ASSESSMENT

VERIFY WHETHER MANUFACTURER DEMONSTRATED CONFORMITY WITH ESSENTIAL REQUIREMENTS

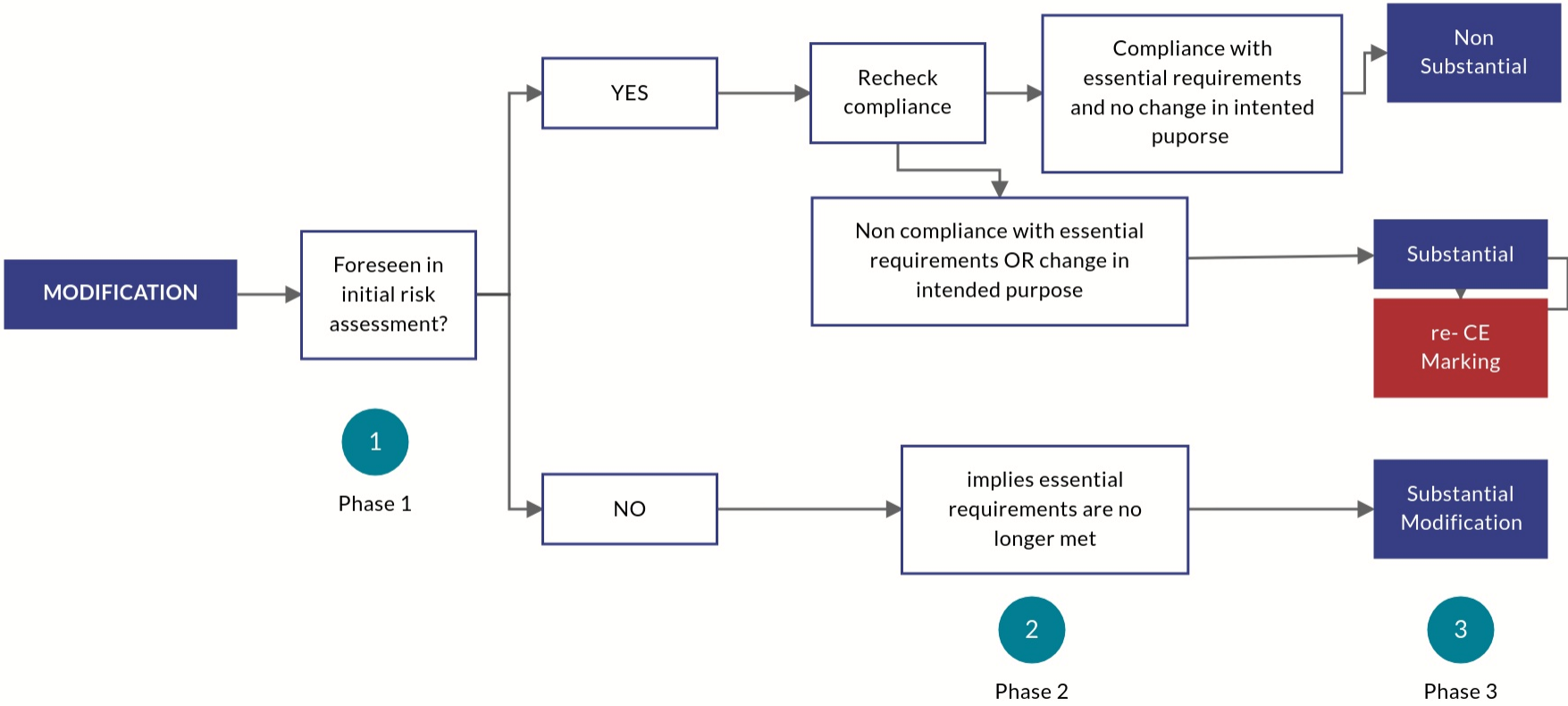
- CE Marking?
- Regular Security Updates?
- Free from vulnerabilities in the European Vulnerability Database?
- Security Tests

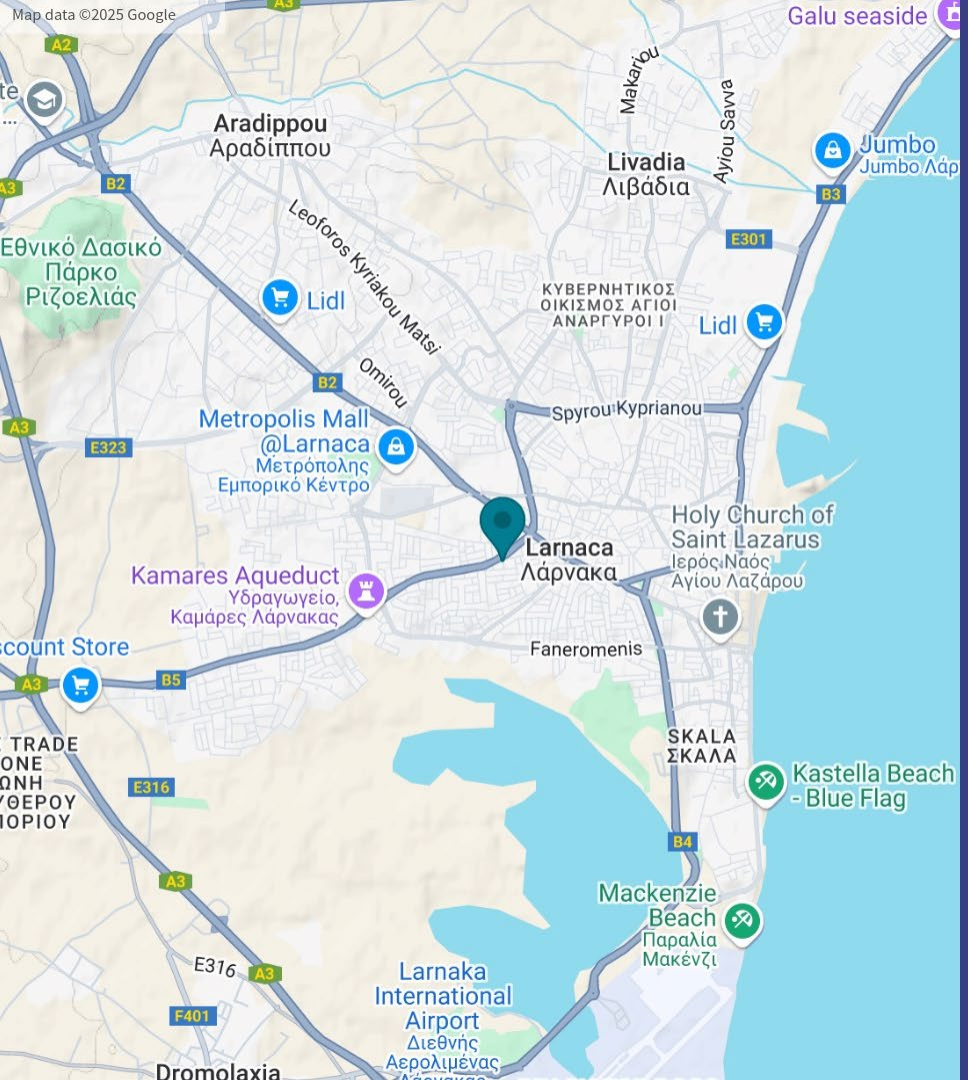
VULNERABILITY HANDLING OBLIGATIONS APPLY TO COMPONENTS

IDENTIFIED VULNERABILITIES

- Report vulnerabilities to manufacturers/mainteners of components
- Address & Remediate
- Provide security fixes

RISK ASSESSMENT & SUBSTANTIAL MODIFICATION





CONTACT US

Konstantinou Palaiologou 33, The Square, 2nd Floor,
6036 Larnaca, Cyprus (HQ)

+357 24 323333

info@raphael.legal

info@privacyminders.com

https://raphael.legal/

https://www.privacyminders.com/