

GDPR Compliance Report

Port Management System

LEI - SEM5 - PI 25/26

TURMA 3DE

GRUPO 05

Document Version: 1.0

Date: October 26, 2025

Project: Port Visit Notification and Management System

Domain: Port Management, Vessel Operations, Cargo Handling

Executive Summary

This report analyzes the current port management system implementation from a General Data Protection Regulation (GDPR) perspective. The system processes personal data from multiple stakeholders including shipping agents, port authority staff, vessel crew members, and company representatives. While basic role-based access control is implemented, significant GDPR compliance gaps currently exist regarding data encryption, consent management, data retention policies, and subject rights fulfillment.

1. Current Implementation

1.1. Personal Data Identified in the System

The system currently processes the following categories of personal data:

A. User Accounts (Domain/Users/User.cs)

- **Personal Identifiers:**
 - `UserId` (Guid)
 - `Name` (string)
 - `Email` (string)
 - `OrganizationId` (organizational affiliation)
- **GDPR Classification:** Basic identity data
- **Legal Basis:** Likely **Contract** (B2B relationship) or **Legitimate Interest** (port operations)
- **Current Implementation:** No explicit consent mechanism, no data retention policy

B. Staff Members (Domain/HumanResources/StaffMember.cs)

- **Personal Identifiers:**

- **MecanographicNumber** (unique employee identifier)
- **ShortName** (name/alias)
- **Email** (contact information)
- **Phone** (contact information)
- **Status** (employment status)
- **StartHour / EndHour** (work schedule)
- **Qualifications** (professional certifications)
- **GDPR Classification:** Employee data (subject to stricter protection under labor law)
- **Legal Basis: Contract** (employment contract) + **Legal Obligation** (safety/security requirements)
- **Sensitive Aspect:** Work schedules and qualifications may reveal health/ability status indirectly

C. Organization Representatives (Domain/Organizations/Representative.cs)

- **Personal Identifiers:**
 - **RepresentativeId** (Guid)
 - **Name** (full name)
 - **CitizenId** (national ID number - **HIGHLY SENSITIVE**)
 - **Nationality** (ISO 3166-1 alpha-2 code)
 - **Email** (contact)
 - **Phone** (contact)
 - **IsActive** (status)
 - **CreatedAt** (timestamp)
- **GDPR Classification: Special Category Data** (CitizenId is a government-issued identifier)
- **Legal Basis: Contract** (business representative) + **Legitimate Interest** (KYC/compliance)
- **Major Risk:** CitizenId storage without encryption violates GDPR Article 32 (Security of Processing)

D. Vessel Crew Members (Domain/Visits/Crew/CrewMember.cs)

- **Personal Identifiers:**
 - **CrewMemberId** (Guid)
 - **Name** (full name)
 - **CitizenId** (national ID/passport number - **HIGHLY SENSITIVE**)
 - **Nationality** (ISO 3166-1 alpha-2 code)
 - **VesselVisitNotificationId** (links to specific vessel visit)
- **GDPR Classification: Special Category Data + International Transfer Concerns**
- **Legal Basis: Legal Obligation** (maritime security regulations: ISPS Code, IMO requirements)
- **Special Concern:** Crew members are often non-EU citizens; data transfer outside EU requires safeguards

E. Captain Data (Domain/Visits/VesselVisitNotification.cs)

- **Personal Identifiers:**
 - **CaptainName** (full name)
 - **CaptainCitizenId** (passport/ID number - **HIGHLY SENSITIVE**)
 - **CaptainNationality** (ISO 3166-1 alpha-2 code)
- **GDPR Classification: Special Category Data**
- **Legal Basis: Legal Obligation** (maritime law, port security)

F. Organizations (Domain/Organizations/Organization.cs)

- **Corporate Data (Limited Personal Data):**
 - **LegalName** (company name)
 - **TaxNumber** (VAT/Tax identification - may link to individual in sole proprietorships)
 - **AddressLine** (business address)
 - Representatives (collection of Representative entities - see C above)
- **GDPR Note:** While primarily B2B data, sole proprietorships and partnerships may have personal data embedded in company names and tax numbers.

1.2. Data Processing Activities

The system performs the following data processing activities:

1. **User Registration and Authentication** (Users, Representatives)
2. **Staff Management** (StaffMember CRUD operations)
3. **Vessel Visit Notification Submission** (VVN creation with captain and crew data)
4. **VVN Approval/Rejection Workflow** (DecisionLog tracks officer actions)
5. **Audit Logging** (DecisionLog records who approved/rejected VVNs)
6. **Role-Based Access Control** (CallerContext enforces authorization)

1.3. GDPR Principles vs. Current Implementation

GDPR Principle	Current Implementation	Compliance Status
Lawfulness, Fairness, Transparency	No privacy policy, no consent mechanisms	✗ Non-Compliant
Purpose Limitation	No documented data processing purposes	⚠ Partial (implicit from domain)
Data Minimisation	Collects necessary data for port operations	<input checked="" type="checkbox"/> Compliant
Accuracy	Update methods exist for contact info	<input checked="" type="checkbox"/> Compliant
Storage Limitation	No data retention policy implemented	✗ Non-Compliant

GDPR Principle	Current Implementation	Compliance Status
Integrity and Confidentiality	No encryption at rest, HTTPS assumed	⚠ Partial
Accountability	Basic audit logging (DecisionLog)	⚠ Partial

2. Technical Implementations Related to GDPR Matters

2.1. Implemented GDPR-Related Features

A. Role-Based Access Control (RBAC)

File: Application/Security/CallerContext.cs

```
public enum AppRole
{
    Unknown = 0,
    ShippingAgentRep = 1,
    PortAuthorityOfficer = 2,
    Admin = 3
}
```

- GDPR Relevance:** Article 32 (Security of Processing) requires access controls
- Current Status:** Basic role-based authorization implemented
- Gaps:**
 - No attribute-based access control (ABAC) for fine-grained permissions
 - No organizational data isolation (ShippingAgentRep can see all data, not just their organization)
 - No data access logging (who accessed which personal data when)

B. Audit Logging for Critical Decisions

File: Domain/Visits/DecisionLog.cs

```
public class DecisionLog
{
    public Guid DecisionLogId { get; private set; }
    public Guid VvnId { get; private set; }
    public UserId OfficerId { get; private set; }
    public string Decision { get; private set; }
    public DateTime DecisionTimestamp { get; private set; }
    public string? DockAssignmentId { get; private set; }
    public string? Reason { get; private set; }
    public string? Notes { get; private set; }
}
```

- GDPR Relevance:** Article 30 (Records of Processing Activities)

- **Current Status:** Approval/rejection decisions are logged with officer ID and timestamp
- **Gaps:**
 - Only captures decision events, not data access/modification events
 - No immutability guarantees (logs could be modified)
 - No log retention policy

C. Data Update Capabilities

File: Domain/HumanResources/StaffMember.cs

```
public void UpdateContactInfo(string email, string phone)
{
    if (string.IsNullOrWhiteSpace(email)) throw new ArgumentException("Email is required.", nameof(email));
    if (string.IsNullOrWhiteSpace(phone)) throw new ArgumentException("Phone is required.", nameof(phone));
    Email = email.Trim();
    Phone = phone.Trim();
}
```

- **GDPR Relevance:** Article 16 (Right to Rectification)
- **Current Status:** Contact information can be updated
- **Gaps:** No audit trail of what was changed, by whom, and when

D. Soft Delete / Deactivation Mechanism

File: Domain/Organizations/Representative.cs

```
public void Deactivate() => IsActive = false;
public void Activate() => IsActive = true;
```

- **GDPR Relevance:** Article 17 (Right to Erasure / "Right to be Forgotten")
- **Current Status:** Representatives can be deactivated (soft delete)
- **Gaps:**
 - No actual data deletion (only status flag)
 - No anonymization/pseudonymization
 - No hard delete capability for GDPR erasure requests

2.2. Partially Implemented / Needs Improvement

A. Organizational Data Isolation

File: Application/Security/CallerContext.cs

```
public sealed class CallerContext
{
```

```

public Guid UserId { get; }
public Guid? OrgId { get; } // Organization ID tracked
public AppRole Role { get; }
}

```

- **Current State:** User's organization is tracked in CallerContext
- **Missing Implementation:** Controllers don't enforce organizational data isolation
- **GDPR Impact:** Shipping agents could potentially access competitors' data (confidentiality breach)

B. Data Validation

File: Multiple domain entities

- **Current State:** Basic validation (required fields, format checks)
- **Missing:** No validation for CitizenId format (varies by country), no Email format validation
- **GDPR Impact:** Invalid data persisted violates Article 5(1)(d) (Accuracy principle)

2.3. Not Implemented / Critical Gaps

A. Data Encryption at Rest

- **Current State:** No encryption implementation found in codebase
- **Risk:** CitizenId, Email, Phone stored in plaintext in database
- **GDPR Violation:** Article 32 (Security of Processing) requires "encryption of personal data"
- **Recommendation:** Implement column-level encryption for sensitive fields (CitizenId, TaxNumber)

B. Consent Management

- **Current State:** No consent tracking mechanism
- **Risk:** No legal basis documented for data processing
- **GDPR Violation:** Article 6 (Lawfulness of Processing) requires valid legal basis
- **Recommendation:** Add **Consent** entity with:
 - Data subject ID
 - Purpose of processing
 - Timestamp
 - Consent granted/withdrawn status

C. Data Retention and Deletion

- **Current State:** No automated data deletion or retention policies
- **Risk:** Personal data retained indefinitely
- **GDPR Violation:** Article 5(1)(e) (Storage Limitation)
- **Recommendation:** Implement retention policies:
 - Crew data: Delete 90 days after vessel departure
 - Inactive users: Anonymize after 2 years of inactivity
 - DecisionLogs: Archive after 5 years (legal requirement)

D. Data Portability

- **Current State:** No export functionality
- **Risk:** Cannot fulfill Article 20 (Right to Data Portability) requests
- **Recommendation:** Implement API endpoint to export user's data in structured JSON/XML format

E. Data Breach Notification

- **Current State:** No breach detection or notification mechanism
 - **Risk:** Cannot comply with 72-hour breach notification requirement
 - **GDPR Violation:** Article 33 (Notification of Personal Data Breach to Supervisory Authority)
 - **Recommendation:** Implement security logging + alerting system
-

3. Future Problems with Current Solution

3.1. Critical Risks

Risk 1: CitizenId Exposure via Data Breach

- **Probability:** High (no encryption at rest)
- **Impact:** Severe (identity theft, fraud)
- **GDPR Fine:** Up to €20 million or 4% of annual global turnover (Article 83)
- **Scenario:** Database backup stolen → 10,000 crew member passport numbers exposed
- **Mitigation Required:**
 - Encrypt CitizenId using AES-256
 - Implement HMAC-based hashing for searchability
 - Restrict CitizenId access to authorized personnel only

Risk 2: Lack of International Data Transfer Safeguards

- **Probability:** High (crew members are international)
- **Impact:** Severe (GDPR violations for non-EU transfers)
- **Legal Issue:** Article 44-50 (Transfers of Personal Data to Third Countries)
- **Scenario:** Crew data from non-EU nationals transferred to cloud provider in US without Standard Contractual Clauses (SCCs)
- **Mitigation Required:**
 - Implement SCCs with cloud providers
 - Data residency controls (store EU citizen data in EU data centers)
 - Privacy Shield replacement compliance (EU-US Data Privacy Framework)

Risk 3: Inability to Fulfill Subject Access Requests (SARs)

- **Probability:** High (no SAR process implemented)
- **Impact:** Moderate (€10-20 million fine)
- **Legal Issue:** Article 15 (Right of Access by Data Subject)
- **Scenario:** Crew member requests all data held about them → no automated way to extract data → 1-month deadline missed
- **Mitigation Required:**
 - Implement SAR portal or API endpoint

- Automated data extraction across all entities (User, CrewMember, DecisionLog references)
- Response template generation

3.2. High Risks

Risk 4: No Data Minimization for Historical Records

- **Current Issue:** Old VVNs retain full crew details indefinitely
- **GDPR Issue:** Article 5(1)(c) (Data Minimisation)
- **Scenario:** VVN from 2020 still contains full crew CitizenId numbers (no longer necessary)
- **Mitigation:**
 - Anonymize crew data in VVNs older than 90 days (keep aggregated statistics only)
 - Implement scheduled jobs for data purging

Risk 5: Lack of Pseudonymization

- **Current Issue:** Real names and IDs used everywhere
- **GDPR Issue:** Article 32(1)(a) recommends pseudonymization
- **Scenario:** Analytics queries on production database expose personal data to data analysts
- **Mitigation:**
 - Generate pseudonymous IDs for analytics
 - Create anonymized reporting database (separate from operational DB)

Risk 6: Missing Privacy-by-Design

- **Current Issue:** No GDPR considerations in system design
- **GDPR Issue:** Article 25 (Data Protection by Design and Default)
- **Scenario:** New feature added (e.g., crew photo upload) without privacy impact assessment → personal data exposure
- **Mitigation:**
 - Conduct Data Protection Impact Assessment (DPIA) for all new features
 - Default privacy settings (e.g., hide staff phone numbers unless explicitly shared)

3.3. Moderate Risks

Risk 7: No Transparency for Data Subjects

- **Current Issue:** No privacy policy, no data processing notices
- **GDPR Issue:** Article 13 (Information to be Provided)
- **Mitigation:**
 - Create privacy policy accessible at [/privacy-policy](#)
 - Display data processing notices at data collection points (e.g., "Your CitizenId is collected for maritime security compliance")

Risk 8: Shared Representative Accounts

- **Current Issue:** Multiple shipping agents may share a Representative account
- **GDPR Issue:** Article 32 (Lack of individual accountability)

- **Mitigation:**
 - Enforce one Representative = one physical person
 - Multi-factor authentication (MFA)
 - Session logging per individual
-

4. Things That Need to Be Improved

4.1. Immediate Actions (0-3 months)

Priority 1: Encrypt Sensitive Personal Data

- **Implementation:**

```
// Add to Domain entities
[EncryptedColumn] // Custom attribute
public string CitizenId { get; private set; }
```

- **Technologies:**

- SQL Server: Transparent Data Encryption (TDE) or Always Encrypted
- Application-level: .NET Data Protection API

- **Timeline:** 1 month

Priority 2: Implement Data Access Logging

- **Implementation:**

- Add **AuditLog** entity:

```
public class AuditLog
{
    public Guid AuditLogId { get; set; }
    public Guid UserId { get; set; }
    public string Action { get; set; } // READ, UPDATE, DELETE
    public string EntityType { get; set; } // "CrewMember",
    "Representative"
    public Guid EntityId { get; set; }
    public DateTime Timestamp { get; set; }
    public string? IpAddress { get; set; }
}
```

- Middleware to capture all controller actions

- **Timeline:** 2 weeks

Priority 3: Organizational Data Isolation

- **Implementation:**

- Modify queries to filter by **CallerContext.OrgId**:

```
var vvns = await _context.VesselVisitNotifications
    .Where(v => v.OrganizationId == callerContext.OrgId)
    .ToListAsync();
```

- **Timeline:** 1 week

4.2. Short-Term Actions (3-6 months)

Priority 4: Data Retention Policy

- **Implementation:**

- Add **RetentionPolicy** configuration:

```
"DataRetention": {
    "CrewMembers": "90days",
    "InactiveUsers": "2years",
    "DecisionLogs": "5years"
}
```

- Scheduled background job (Hangfire or Quartz.NET):

```
public class DataRetentionJob
{
    public void Execute()
    {
        // Anonymize crew members from VVNs older than 90 days
        var oldVvns = _context.VesselVisitNotifications
            .Where(v => v.Etd < DateTime.UtcNow.AddDays(-90))
            .Include(v => v.CrewMembers);

        foreach (var vvn in oldVvns)
        {
            foreach (var crew in vvn.CrewMembers)
            {
                crew.Anonymize(); // Name → "REDACTED", CitizenId →
                *****
            }
        }
        await _context.SaveChangesAsync();
    }
}
```

- **Timeline:** 2 months

Priority 5: Subject Access Request (SAR) API

- **Implementation:**

- New controller endpoint:

```
[HttpGet("api/gdpr/my-data")]
public async Task<IActionResult> GetMyData()
{
    var userId = CallerContext.UserId;
    var myData = new
    {
        User = await _context.Users.FindAsync(userId),
        RepresentativeData = await _context.Representatives
            .Where(r => r.Email == user.Email).ToListAsync(),
        CrewRecords = await _context.CrewMembers
            .Where(c => c.CitizenId == user.CitizenId).ToListAsync(),
        VvnHistory = await _context.VesselVisitNotifications
            .Where(v => v.SubmittedById == userId).ToListAsync()
    };
    return Ok(myData); // Export as JSON
}
```

- **Timeline:** 1 month

Priority 6: Consent Management System

- **Implementation:**

- Add **Consent** entity:

```
public class Consent
{
    public Guid ConsentId { get; set; }
    public Guid DataSubjectId { get; set; } // UserId or
    RepresentativeId
    public string Purpose { get; set; } // "VVN_PROCESSING",
    "MARKETING"
    public bool IsGranted { get; set; }
    public DateTime GrantedAt { get; set; }
    public DateTime? WithdrawnAt { get; set; }
    public string LegalBasis { get; set; } // "CONSENT", "CONTRACT",
    "LEGAL_OBLIGATION"
}
```

- **Timeline:** 2 months

4.3. Medium-Term Actions (6-12 months)

Priority 7: Data Protection Impact Assessment (DPIA)

- **Process:**

1. Identify high-risk processing activities (crew data collection, CitizenId storage)
 2. Assess necessity and proportionality
 3. Identify risks to data subjects
 4. Propose mitigation measures
 5. Document in DPIA report
- **Timeline:** 3 months (ongoing for new features)

Priority 8: Privacy Policy and Transparency

- **Implementation:**
 - Create comprehensive privacy policy covering:
 - Data controller identity (Port Authority)
 - Data processing purposes
 - Legal basis for each processing activity
 - Data retention periods
 - Data subject rights
 - Contact details for Data Protection Officer (DPO)
 - Display at registration and data collection points
- **Timeline:** 1 month

Priority 9: Right to Erasure Implementation

- **Implementation:**
 - Add `DeleteMyData` endpoint:
- ```
[HttpDelete("api/gdpr/delete-my-data")]
public async Task<IActionResult> DeleteMyData()
{
 // Check if legal obligations prevent deletion (e.g., ongoing VVN)
 var activeVvns = await _context.VesselVisitNotifications
 .Where(v => v.SubmittedById == CallerContext.UserId && v.State
 != VVNState.REJECTED)
 .AnyAsync();

 if (activeVvns)
 return BadRequest("Cannot delete data while active VVNs
exist");

 // Hard delete or anonymize
 var user = await _context.Users.FindAsync(CallerContext.UserId);
 _context.Users.Remove(user);
 await _context.SaveChangesAsync();

 return Ok("Data deleted successfully");
}
```

- **Timeline:** 1 month

## **Priority 10: Breach Detection and Notification**

- **Implementation:**
    - Integrate security monitoring (e.g., Azure Sentinel, Splunk)
    - Automated alerts for:
      - Mass data exports
      - Unauthorized access attempts
      - Database query anomalies
    - Breach notification workflow:
      1. Detection → 2. Investigation → 3. Containment → 4. Notify supervisory authority (72h) → 5. Notify affected data subjects
  - **Timeline:** 4 months
- 

## **5. Other References: Port Management, Private Data, and GDPR**

### **5.1. Regulatory Framework for Port Operations**

#### **A. Maritime Security Regulations**

- **International Ship and Port Facility Security (ISPS) Code**
  - Requires collection of crew and passenger data for security screening
  - Legal basis for processing captain and crew CitizenId under GDPR Article 6(1)(c) (Legal Obligation)
  - Reference: IMO SOLAS Chapter XI-2
- **EU Regulation 725/2004 (Maritime Security)**
  - Implements ISPS Code in EU law
  - Mandates retention of vessel visit records for security purposes
  - Potential conflict with GDPR storage limitation → **Legal obligation overrides** (Article 6(1)(c))

#### **B. Customs and Border Control**

- **EU Customs Code (Regulation 952/2013)**
  - Requires cargo manifests and crew declarations
  - Justifies processing of crew data for customs clearance
- **Schengen Borders Code**
  - Non-EU crew members entering Schengen Area → passport data processed
  - Data sharing with border authorities (Article 6(1)(c) - Legal Obligation)

### **5.2. GDPR-Specific Guidance for Port Operations**

#### **A. European Data Protection Board (EDPB) Opinions**

- **Guidelines 3/2019 on Processing of Personal Data through Video Devices**

- Relevant for port CCTV systems (not yet in scope, but future consideration)
- **Guidelines 2/2019 on Article 49 GDPR (International Data Transfers)**
  - Critical for crew data from non-EU nationals
  - Derogations for specific situations (Article 49(1)(d) - Important public interest in maritime security)

## B. Data Sharing with Authorities

- **Port State Control (PSC) Inspections**
  - Sharing crew data with national maritime authorities
  - Legal basis: Article 6(1)(c) + Article 6(1)(e) (Public interest / Official authority)
  - No separate consent required
- **Law Enforcement Requests**
  - Police/customs may request crew data for investigations
  - Article 23 GDPR allows restrictions on data subject rights for law enforcement
  - Must log and document all disclosures

## 5.3. Private Companies and B2B Data Processing

### A. Shipping Agents and Logistics Operators

- **GDPR Role:** Joint Controllers with Port Authority
  - Both parties determine purposes and means of processing
  - Requires Data Processing Agreement (Article 26)
- **Current Gap:** No contract defining:
  - Who is responsible for responding to SARs
  - Who notifies data subjects of breaches
  - Data retention responsibilities
- **Recommendation:** Draft **Joint Controller Agreement** covering:

1. Port Authority responsibilities:
  - Provides technical infrastructure
  - Handles VVN approval/rejection
  - Responds to crew data SARs
2. Shipping Agent responsibilities:
  - Collects crew data lawfully
  - Obtains consent where required
  - Updates/corrects data upon request
3. Shared responsibilities:

- Breach notification (both parties notify within 24h)
- Data retention (delete crew data 90 days post-departure)

## B. Representatives and Sole Traders

- **Issue:** Representative CitizenId is personal data
- **Scenario:** Shipping agent is a sole proprietorship → owner's personal data mixed with company data
- **GDPR Implication:** Cannot justify processing sole trader's CitizenId under "legitimate interest" alone
- **Solution:**
  - Obtain explicit consent for CitizenId processing
  - Offer alternative authentication (e.g., business tax number only, no CitizenId)

## 5.4. Staff Working at the Port

### A. Employee Data Protection

- **StaffMember Entity:** Contains employment data (work schedule, qualifications, contact info)
- **Legal Basis:** Employment contract (Article 6(1)(b))
- **Special Considerations:**
  - **Work schedules:** May indirectly reveal health issues (e.g., reduced hours)
  - **Qualifications:** Certifications may indicate disabilities (e.g., hearing impairment → no crane operator license)
  - **Phone/Email:** Can employees refuse to provide personal contact info?
- **Recommendations:**
  - Clear policy: Work phone/email only (no personal contact info unless consented)
  - Data minimization: Only store qualifications relevant to current role
  - Employee privacy notice: Inform staff how their data is used (scheduling, payroll, emergency contact)

### B. Access Control for HR Data

- **Current Risk:** Port Authority Officers may have access to all staff data
- **GDPR Requirement:** Need-to-know principle (Article 32)
- **Solution:**
  - Separate HR role (**HRManager**) with exclusive access to StaffMember data
  - Port Authority Officers only see staff assignments, not personal details

## 5.5. Vessel Crew and Captains

### A. International Data Transfers

- **Scenario:** Vessel flagged in Panama, crew from Philippines, visiting Portuguese port
- **GDPR Issue:** Crew data transferred outside EU when VVN is processed
- **Solutions:**

1. **Article 49(1)(d) Derogation:** Public interest in maritime security (preferred)
2. **Standard Contractual Clauses (SCCs):** If data shared with non-EU vessel operators
3. **Adequacy Decisions:** Check if crew's home country has EU adequacy decision (e.g., UK, Japan)

## B. Crew Data Retention

- **Regulatory Conflict:**
  - **ISPS Code:** May require 5-year retention for security records
  - **GDPR:** Storage limitation principle
- **Resolution:**
  - **Operational data:** Delete crew details 90 days after departure
  - **Security incidents:** Retain indefinitely if crew involved in security event (legal obligation)
  - **Anonymized statistics:** Keep aggregated crew count, nationalities (no personal identifiers)

## C. Captain's Role

- **Dual Status:** Captain is both:
  1. Data subject (their personal data is collected)
  2. Data controller (responsible for crew data on behalf of vessel operator)
- **GDPR Implication:** Captain must:
  - Inform crew that their data will be shared with port authorities
  - Ensure crew data is accurate before submitting VVN
  - Facilitate crew members' GDPR rights (e.g., access, rectification)
- **Recommendation:** Provide captain with crew privacy notice template in multiple languages

## 5.6. Third-Party Data Processors

### A. Cloud Hosting Providers

- **If using Azure, AWS, Google Cloud:**
  - GDPR Role: Data Processor (Article 28)
  - Requirement: Data Processing Agreement (DPA) must exist
  - Check: Does DPA cover sub-processors? Data residency? Breach notification?

### B. Email Service Providers

- **If sending notifications via SendGrid, Mailgun, etc.:**
  - Personal data (email addresses) shared with processor
  - Must have DPA in place
  - Ensure email service has EU data centers

---

## 6. Recommended GDPR Compliance Roadmap

## **Phase 1: Foundation (Months 1-3)**

1. Conduct full data inventory
2. Appoint Data Protection Officer (DPO) or GDPR compliance lead
3. Draft Privacy Policy and Data Processing Notices
4. Implement encryption for CitizenId and sensitive fields
5. Enable organizational data isolation in controllers
6. Implement data access audit logging

## **Phase 2: Core Compliance (Months 4-6)**

7. Deploy consent management system
8. Implement Subject Access Request (SAR) API
9. Create data retention policy and automated purging
10. Draft Data Processing Agreements with shipping agents
11. Establish breach detection and notification procedures

## **Phase 3: Advanced Features (Months 7-12)**

12. Implement Right to Erasure (hard delete + anonymization)
13. Data Portability API (export in machine-readable format)
14. Conduct Data Protection Impact Assessment (DPIA) for high-risk processing
15. Pseudonymization for analytics and reporting
16. Multi-language privacy notices for international crew

## **Phase 4: Continuous Improvement (Ongoing)**

17. Quarterly GDPR compliance audits
  18. Staff training on data protection principles
  19. Monitor EDPB guidance and ECJ rulings for updates
  20. Privacy-by-design reviews for all new features
- 

## **7. Conclusion**

The current port management system processes significant volumes of personal data, including highly sensitive national identifiers (CitizenId) for crew members and company representatives. While basic role-based access control and decision audit logging are implemented, **critical GDPR compliance gaps exist:**

### **Key Risks:**

1. **No encryption at rest** for CitizenId and other sensitive data
2. **No data retention policy** → indefinite storage violates storage limitation
3. **No consent management** → unclear legal basis for processing
4. **Inability to fulfill data subject rights** (access, erasure, portability)
5. **No international data transfer safeguards** for non-EU crew members

### **Priority Actions:**

1. **Immediate:** Encrypt sensitive personal data (CitizenId, TaxNumber)

2. **Short-term:** Implement data access logging and organizational data isolation
3. **Medium-term:** Deploy SAR API, consent management, and data retention automation
4. **Long-term:** Conduct DPIA, establish breach response procedures, train staff

## **Legal Justifications:**

- Crew/captain data: **Legal obligation** (ISPS Code, EU Regulation 725/2004)
- Staff data: **Employment contract** + legal obligations (safety/security)
- Organization/representative data: **Contract** (B2B relationship) + **Legitimate interest** (KYC)
- User accounts: **Contract** or **Legitimate interest** (port operations)

By following the recommended roadmap, the system can achieve **full GDPR compliance within 12 months** while maintaining operational efficiency for port management activities.

---

## References

1. **GDPR (Regulation 2016/679):** <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
2. **EDPB Guidelines:** [https://edpb.europa.eu/our-work-tools/general-guidance\\_en](https://edpb.europa.eu/our-work-tools/general-guidance_en)
3. **IMO ISPS Code:** <https://www.imo.org/en/OurWork/Security/Pages/SOLAS-XI%20ISPS%20Code.aspx>
4. **EU Regulation 725/2004 (Maritime Security):** <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32004R0725>
5. **EU Customs Code:** [https://taxation-customs.ec.europa.eu/customs-4/union-customs-code\\_en](https://taxation-customs.ec.europa.eu/customs-4/union-customs-code_en)
6. **Standard Contractual Clauses (SCCs):** [https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en)