GDPR Compliance Report - Sprint B

Port Management System

LEI - SEM5 - PI 25/26

TURMA 3DE

GRUPO 05

Document Version: 2.0
Date: November 22, 2025
Project: Port Visit Notification and Management System
Sprint: Sprint B - Authentication, Authorization, and GDPR Awareness
Previous Version: GDPR_Compliance_Report_SprintA.pdf

Executive Summary

This report provides a comprehensive GDPR compliance analysis for the Port Management System at the end of Sprint B. Building upon the Sprint A foundation, this document addresses the authentication, authorization, and data protection features introduced in Sprint B while maintaining visibility of the core data processing activities identified in Sprint A.

The system processes personal data from multiple stakeholders including shipping agents, port authority staff, vessel crew members, company representatives, and now includes external authentication through Google OAuth. Sprint B introduces significant changes to how users authenticate and access the system, creating new data processing activities and associated GDPR obligations.

Key Sprint B Additions:

- External IAM Integration (Google OAuth) - US 3.2.1
- User Activation via Email - US 3.2.5, 3.2.6
- Token-Based Session Management - US 3.2.3
- Enhanced Role-Based Access Control (RBAC/ABAC) - US 3.2.4
- GDPR Awareness and Breach Response - US 3.6.1, 3.6.2

Overall GDPR Compliance Status:

- ☑ **Strengths:** OAuth eliminates password storage risks, organizational data isolation, basic audit logging
- ⚠ **Moderate Gaps:** No encryption at rest for sensitive data, token storage vulnerabilities, incomplete audit trails
- ✖ **Critical Gaps:** No data retention policy, no breach notification procedures, no Subject Access Request (SAR) mechanism, missing Data Processing Agreements

---

1. Current Implementation - Personal Data Inventory

1.1. Personal Data Identified in the System (Sprint A + Sprint B)

The system processes the following categories of personal data across all operational modules:

A. User Accounts (Sprint A + Sprint B Enhanced)

Sprint A Data:

- `UserId` (Guid - internal identifier)
- `Name` (string)
- `Email` (string)
- `OrganizationId` (organizational affiliation)

Sprint B Additions:

- `GoogleUserId` (Google OAuth sub claim - external identifier)
- `ActivationToken` (Guid - temporary authentication credential)
- `TokenExpiry` (DateTime - token expiration timestamp)
- `ActivationStatus` (Enum: Pending, Activated, Expired, Revoked)
- `ActivatedAt` (DateTime - account activation timestamp)
- `LastLogin` (DateTime - last authentication event)

GDPR Classification: Basic identity data + authentication credentials

Legal Basis:

- Sprint A: Contract (B2B relationship) or Legitimate Interest
- Sprint B: Contract (necessary for system access via OAuth)

New Risks: Google account compromise, activation email interception, token theft via XSS

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

Sprint B Impact: Access to staff data now controlled via RBAC/ABAC - only authorized roles can view

---

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

Sprint B Impact: Representatives now authenticate via Google OAuth (if given system access)

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

Sprint B Impact: Access to crew CitizenId now requires authentication + proper role (PortAuthorityOfficer or assigned ShippingAgentRep)

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)

Sprint B Impact: Same access controls as crew data

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)

GDPR Note: While primarily B2B data, sole proprietorships may have personal data embedded in company names and tax numbers

---

G. NEW - Google OAuth Data (Sprint B)

Data Received from Google OAuth:

- `sub` (Google User ID)
- `email` (verified email address)
- `email_verified` (boolean)
- `name` (full name from Google profile)
- `picture` (profile picture URL - not stored)
- `given_name`, `family_name` (not stored)

GDPR Classification: Basic identity data

Legal Basis: Article 6(1)(b) - Contract (necessary for authentication)

Third-Party Processor: Google LLC

- Privacy Policy: https://policies.google.com/privacy
- International Transfer: EU-US Data Privacy Framework (adequacy decision)
- **Gap:** No formal Data Processing Agreement (DPA) in place

---

H. NEW - JWT Session Tokens (Sprint B)

Data in JWT Payload:

- `userId` (internal identifier)
- `email` (user email)
- `name` (user full name)
- `role` (ShippingAgentRep, PortAuthorityOfficer, Admin)
- `orgId` (organization identifier - if applicable)
- `iat` (issued at timestamp)
- `exp` (expiration timestamp)

GDPR Classification: Authentication credentials containing personal identifiers

Legal Basis: Article 6(1)(b) - Contract (necessary for session management)

Storage Location: Browser localStorage (XSS vulnerability - see Section 3)

Retention: 60 minutes (access token), 7 days (refresh token)

I. NEW - Email Activation Data (Sprint B)

Data Elements:

- `ActivationToken` (unique identifier in email link)
- `UserEmail` (recipient of activation email)
- `AssignedRole` (initial role)
- `TokenExpiry` (7-day expiration)

GDPR Classification: Authentication credentials

Legal Basis: Article 6(1)(b) - Contract (account provisioning)

Third-Party Processor: Gmail SMTP (Google LLC)

- **Gap:** No DPA for email service
- **Gap:** Unknown retention period for sent emails in Gmail

1.2. Data Processing Activities (Consolidated Sprint A + Sprint B)

Processing Activity	Personal Data	Legal Basis	Data Subjects	Sprint
User Registration	Name, email, organization	Contract 6(1)(b)	All users	A
Google OAuth Authentication	Email, name, Google ID	Contract 6(1)(b)	All users	B
User Activation via Email	Email, activation token, role	Contract 6(1)(b)	New users	B
JWT Session Management	UserId, email, name, role, orgId	Contract 6(1)(b)	Authenticated users	B
Role Assignment & Authorization	UserId, role, orgId	Legitimate Interest 6(1)(f)	Internal users	B
Staff Management	Employee data, qualifications, schedule	Contract 6(1)(b) + Legal Obligation 6(1)(c)	Port staff	A
VVN Submission	Captain/crew CitizenId, nationality	Legal Obligation 6(1)(c)	Crew members	A

Processing Activity	Personal Data	Legal Basis	Data Subjects	Sprint
VVN Approval/Rejection	VVN data access, decision logs	Legal Obligation 6(1)(c)	Shipping agents	A
Audit Logging	UserId, action, timestamp, IP	Legal Obligation 6(1)(c)	All users	A+B

1.3. Third-Party Data Processors

Processor	Role	Data Processed	DPA Status	Sprint
Google OAuth	Authentication provider	Email, name, Google ID	✗ Missing	B
Gmail SMTP	Email delivery	Activation emails with tokens	✗ Missing	B
Cloud Hosting	Infrastructure	All system data	⚠ Assumed	A
Email Service Provider	Notifications	User emails	⚠ Assumed	A

Critical Gap: No formal Data Processing Agreements (Article 28) with Google services

2. Sprint B GDPR-Related Technical Implementations

2.1. Google OAuth Authentication (US 3.2.1)

Purpose: Replace password-based authentication with external IAM provider

Data Flow:

1. User clicks "Login with Google"
2. System redirects to Google OAuth consent screen
3. Google authenticates user and asks for consent to share email and name
4. User approves → Google sends authorization code to system
5. System exchanges code for ID token (contains email, name, Google user ID)
6. System verifies email exists in database and loads internal role
7. System issues JWT access token and refresh token
8. User gains access to system based on assigned role

GDPR Considerations:

- **Transparency:** Users must be informed about Google data sharing before OAuth redirect
- **Data Minimization:** Only request necessary OAuth scopes (openid, email, profile)
- **Third-Party Disclosure:** Privacy policy must mention Google as processor
- **Data Controller Responsibility:** System remains controller; Google is processor

Security Measures:

- ☑ Authorization code flow (secure)
- ☑ HTTPS for all OAuth redirects
- ☑ State parameter prevents CSRF attacks
- ✗ **Gap:** No PKCE (Proof Key for Code Exchange) for SPA security
- ✗ **Gap:** No nonce parameter in ID token validation

2.2. User Activation via Email (US 3.2.5, 3.2.6)

Purpose: Controlled user onboarding with email verification

Data Flow:

1. Administrator creates user account with email, name, role
2. System generates unique activation token (7-day validity)
3. System sends email via Gmail SMTP with activation link containing token
4. User clicks link → System redirects to Google OAuth
5. User authenticates with Google
6. System verifies authenticated email matches user account email
7. System activates account (deletes token, sets status to Active)
8. User gains access with assigned role

GDPR Considerations:

- **Data in Transit:** Activation token transmitted via email (HTTPS link, TLS SMTP)
- **Token as Personal Data:** Linked to user identity
- **Retention:** Token deleted after activation or 7-day expiration
- **Breach Risk:** Email interception could enable account hijacking

Security Measures:

- ☑ Tokens expire after 7 days
- ☑ Tokens are single-use (deleted after activation)
- ☑ Email verification via OAuth confirms ownership
- ✗ **Gap:** Tokens not cryptographically signed
- ✗ **Gap:** No rate limiting on activation endpoint
- ✗ **Gap:** No admin notification if activation fails multiple times

---

2.3. JWT Token Management (US 3.2.3)

Purpose: Stateless session management for API authorization

Token Structure:

- **Access Token:** 60-minute lifetime, contains userId, email, name, role, orgId
- **Refresh Token:** 7-day lifetime, used to obtain new access tokens

Data Flow:

1. User authenticates successfully
2. Backend generates signed JWT tokens
3. Tokens stored in browser localStorage
4. Frontend attaches access token to every API request (Authorization header)
5. Backend validates token signature and expiry
6. On expiration, frontend uses refresh token to get new access token
7. On logout, frontend deletes tokens from localStorage

GDPR Considerations:

- **Personal Data in Token:** JWT contains email, name, userId (identifiers)
- **XSS Vulnerability:** localStorage accessible to malicious JavaScript
- **Token Lifetime:** Longer validity increases risk if stolen
- **No Revocation:** Compromised tokens valid until expiration

Security Measures:

- ☑ Short-lived access tokens (60 minutes)
- ☑ HTTPS prevents interception
- ☑ Tokens cryptographically signed (HMAC-SHA256)
- ✗ **Gap:** localStorage is XSS-vulnerable (should use httpOnly cookies for refresh tokens)
- ✗ **Gap:** No token revocation mechanism
- ✗ **Gap:** No audit logging of token usage

2.4. Role-Based and Attribute-Based Access Control (US 3.2.4)

Purpose: Enforce authorization and organizational data isolation

Implementation:

- **Backend:** Authorization handlers check role claims from JWT
- **Backend:** Organizational data filter applies WHERE clause: `orgId = user.orgId` for ShippingAgentRep
- **Frontend:** Route guards prevent UI navigation to unauthorized pages
- **Frontend:** Menu options rendered dynamically based on role

Authorization Rules:

- **ShippingAgentRep:** Can only access own organization's VVNs and resources
- **PortAuthorityOfficer:** Can access all VVNs for approval, all docks/storage areas
- **Admin:** Can manage users, assign roles, access all data

GDPR Considerations:

- **Article 32 Compliance:** Access control ensures confidentiality
- **Organizational Data Isolation:** Prevents competitors from accessing each other's data
- **Audit Logging Required:** Authorization failures should be logged

Security Measures:

- ☑ Backend enforces authorization (frontend guards are UI-only)
- ☑ Organizational data isolation implemented
- ☑ Role claims validated from signed JWT
- ❌ **Gap:** No audit logging of authorization failures (403 Forbidden)
- ❌ **Gap:** No fine-grained permissions beyond role level
- ❌ **Gap:** No role hierarchy (Admin doesn't inherit PortAuthorityOfficer permissions)

2.5. Audit Logging (Sprint A + Sprint B)

Sprint A Implementation:

- Decision logs for VVN approvals/rejections (OfficerId, timestamp, decision, reason)

Sprint B Gaps:

- ❌ No logging of Google OAuth authentication events
- ❌ No logging of user activation attempts
- ❌ No logging of JWT token usage (API access)
- ❌ No logging of authorization failures
- ❌ No logging of data access (who viewed which crew CitizenId)

Article 30 Requirement: Records of processing activities must be maintained

---

3. GDPR Principles vs. Current Implementation

GDPR Principle	Sprint A Status	Sprint B Status	Gap Assessment
Lawfulness, Fairness, Transparency	❌ No privacy policy	⚠ Google OAuth consent partial	Need system privacy policy
Purpose Limitation	⚠ Implicit purposes	⚠ OAuth purposes clear	Document all purposes formally
Data Minimisation	☑ Necessary data collected	⚠ JWT contains more data than needed	Consider opaque tokens
Accuracy	☑ Update methods exist	☑ Google profile data verified	Adequate
Storage Limitation	❌ No retention policy	❌ No retention policy	Critical gap remains
Integrity and Confidentiality	⚠ No encryption at rest	⚠ Token storage vulnerable	Multiple security gaps
Accountability	⚠ Basic audit logging	⚠ Incomplete audit logs	Expand audit coverage

---

4. Sprint B-Specific Risks and Breach Scenarios

4.1. Critical Risk: JWT Token Theft via XSS Attack

Probability: Medium-High

Impact: Severe (session hijacking, data breach)

Scenario:

1. Attacker injects malicious JavaScript via unsanitized input field
2. Script executes in victim's browser and steals access token from localStorage
3. Attacker obtains JWT containing userId, email, name, role, orgId
4. Attacker uses token to impersonate victim for 60 minutes
5. Attacker accesses all data available to victim's role (potentially 500+ crew records if admin)

GDPR Violation: Article 32 (Security of Processing) - failure to protect authentication credentials

Data Breach: YES - unauthorized access to personal data

Notification Required: YES - Article 33 (notify supervisory authority within 72 hours)

Mitigation:

- Immediate: Store refresh tokens in httpOnly cookies (inaccessible to JavaScript)
- Short-term: Implement Content Security Policy (CSP) headers
- Short-term: Sanitize all user inputs
- Medium-term: Token binding (tie tokens to specific browser/device)

4.2. High Risk: Activation Email Interception

Probability: Low-Medium

Impact: Severe (account takeover)

Scenario:

1. Admin creates user account and sends activation email
2. Attacker intercepts email (compromised email account, network sniffing)
3. Attacker clicks activation link before legitimate user
4. Current implementation gap: Email verification happens AFTER OAuth authentication
5. Attacker could potentially activate with own Google account

GDPR Violation: Article 32 (inadequate security measures)

Mitigation:

- Immediate: Enforce email matching (authenticated Google email must match account email)
- Short-term: Reduce token expiration to 24 hours
- Medium-term: IP address logging and anomaly detection
- Medium-term: "Resend activation email" feature (invalidates old token)

4.3. High Risk: Google OAuth Account Compromise

Probability: Low (depends on user's Google security)

Impact: Severe (system access with user's privileges)

Scenario:

1. User's Google account compromised via phishing
2. Attacker logs into Port Management System
3. System authenticates attacker (Google confirms identity)
4. Attacker accesses all data available to victim's role

GDPR Controller Responsibility: Article 24 - controller must implement appropriate measures

Mitigation:

- Short-term: Device fingerprinting (detect new device logins)
- Medium-term: Require MFA for sensitive actions
- Medium-term: Session timeout (auto-logout after inactivity)
- Long-term: Behavioral analytics

4.4. Moderate Risk: JWT Token Not Revocable

Probability: High (inevitable when compromise detected)

Impact: Moderate-Severe (continued unauthorized access)

Scenario:

1. User reports suspicious activity
2. Admin deactivates account in database
3. Attacker's stolen JWT remains valid for 60 minutes
4. Attacker continues accessing data during this window

GDPR Violation: Article 32 - inability to immediately terminate unauthorized access

Mitigation:

- Immediate: Reduce access token lifetime to 15 minutes
- Short-term: Implement token revocation list in Redis
- Medium-term: "Logout all sessions" feature

4.5. Moderate Risk: Gmail SMTP as Uncontrolled Sub-Processor

Probability: N/A (current state)

Impact: Compliance risk (no DPA)

Issue: Activation emails sent via Gmail SMTP without Data Processing Agreement

GDPR Violation: Article 28(3) - processor shall not engage sub-processor without authorization

Privacy Risk: Gmail may retain sent emails indefinitely

Mitigation:

- Immediate: Switch to EU-based transactional email service (SendGrid EU, Mailgun EU)
- Short-term: Establish DPA with email provider
- Alternative: Use SMS for activation codes

---

5. US 3.6.1 Compliance - Personal Data Processing Explanation

5.1. Project Scope and Core Functionalities

What is the Port Management System?

The Port Management System is a digital platform coordinating vessel visits to a maritime port. It connects three key actors:

1. **Shipping Agents** - Submit vessel visit notifications with cargo and crew information
2. **Port Authority Officers** - Review and approve/reject notifications, assign docks
3. **Logistics Operators** - Manage port resources (staff, cranes, storage areas)

Why Personal Data?

- **Security Compliance:** Maritime regulations (ISPS Code) require crew identification
- **Business Operations:** Contact representatives of shipping companies
- **System Access:** Authenticate and authorize users based on their roles

Sprint B Focus: Secure authentication via Google OAuth and role-based access control

---

5.2. Which Personal Data Will Be Processed

Category 1: Authentication & Identity

- Google profile data (email, name, Google user ID)
- User activation tokens (temporary credentials)
- Session tokens (JWT containing userId, email, role)

Category 2: Business Representatives

- Representative names, citizen IDs, nationalities, contact information
- Organizational affiliations

Category 3: Vessel Crew & Captains

- Names, citizen IDs/passport numbers, nationalities
- Associated with specific vessel visits

Category 4: Port Staff

- Employee names, contact information, qualifications, work schedules

Category 5: Administrative Metadata

- User roles, activation status, login timestamps
- Audit logs of approvals/rejections

5.3. How Personal Data Will Be Processed

Processing Activity 1: User Authentication via Google OAuth

Process:

1. User clicks "Login with Google"
2. System redirects to Google (user authenticates with Google)
3. Google asks: "Allow Port Management System to access your email and name?"
4. User approves → Google sends authorization code
5. System exchanges code for ID token (contains email, name)
6. System checks if email exists in database
7. If exists → Load role and generate session token
8. User gains access based on assigned role

Personal Data Flow:

- Collected: Email, name, Google user ID
- Stored: In system database (Users table)
- Transmitted: Browser ↔ Google ↔ System backend (HTTPS encrypted)
- Shared: With Google LLC (authentication provider)

Purpose: User authentication without storing passwords

Legal Basis: Article 6(1)(b) - Performance of Contract

Processing Activity 2: User Activation via Email

Process:

1. Administrator creates user account with email, name, role
2. System generates unique activation token (7-day validity)
3. System sends email with activation link
4. User clicks link → Redirects to Google OAuth
5. User authenticates with Google
6. System verifies Google email matches account email
7. System activates account (deletes token)

Personal Data Flow:

- Collected: Email, activation token, role
- Stored: In database until activation
- Transmitted: Via email (Gmail SMTP), via URL (HTTPS)
- Shared: With Gmail SMTP service

Purpose: Account provisioning and email verification

Legal Basis: Article 6(1)(b) - Performance of Contract

Processing Activity 3: Session Management

Process:

1. User authenticates successfully
2. System generates JWT tokens (access + refresh)
3. Tokens stored in browser localStorage
4. Frontend attaches access token to every API request
5. Backend validates token and processes request
6. Token expires → Frontend uses refresh token
7. Logout → Tokens deleted from browser

Personal Data: UserId, email, name, role, orgId

Purpose: Secure session management and API authorization

Legal Basis: Article 6(1)(b) - Performance of Contract

Processing Activity 4: Authorization Enforcement

Process:

1. User attempts to access feature or data
2. Frontend checks role before rendering page
3. Backend validates role from JWT token
4. For data queries, apply organizational filter (ShippingAgentRep sees only own data)
5. If authorized → Process request
6. If unauthorized → Return "Access Denied"

Purpose: Enforce data isolation and prevent unauthorized access

Legal Basis: Article 6(1)(f) - Legitimate Interest (security)

Processing Activity 5: VVN Submission with Crew Data

Process:

1. Shipping agent submits vessel visit notification
2. Includes cargo manifest and crew list
3. Crew data: Name, CitizenId, Nationality for each crew member
4. Data stored and linked to VVN
5. Port Authority reviews and approves/rejects
6. Decision logged with officer ID and timestamp

Purpose: Maritime security compliance (ISPS Code)

Legal Basis: Article 6(1)(c) - Legal Obligation

5.4. Legal Basis for Each Type of Processing

Processing Activity	Personal Data	Legal Basis	Article 6(1)
Google OAuth Login	Email, name, Google ID	Contract	(b)
User Activation	Email, token, role	Contract	(b)
JWT Sessions	UserId, email, role, orgId	Contract	(b)
Role Assignment	UserId, role, organization	Legitimate Interest	(f)
Crew/Captain Data	CitizenId, nationality	Legal Obligation	(c)
Staff Management	Employee data, schedule	Contract + Legal Obligation	(b) + (c)
Audit Logging	UserId, timestamp, action	Legal Obligation	(c)

Legitimate Interest Assessment (Role Assignment):

- **Purpose:** Prevent unauthorized access to sensitive data (crew CitizenId)
- **Necessity:** Access control is fundamental security measure (Article 32)
- **Balancing Test:** Privacy impact (role metadata) < Security benefit (prevent breaches)
- **Conclusion:** Legitimate interest is appropriate

5.5. How Processing Affects Different Actors

Shipping Agent Representatives:

- ✅ Faster login via Google OAuth (no password management)
- ✅ Organizational data isolation (cannot access competitors' data)
- ⚠️ Google account compromise = system access compromise
- 📋 Rights: Can request data export (activation history, login logs)

Port Authority Officers:

- ✅ Access to all VVNs for approval workflow
- ⚠️ Higher responsibility (broader data access)
- 🔒 Backend audit logs track all approval decisions
- 📋 Subject to employee data protection policies

Administrators:

- ✅ Can onboard users and assign roles
- ⚠️ Admin actions logged (accountability)
- 🔒 Should require MFA (not yet implemented)
- 📋 Must handle activation emails securely

Crew Members (Indirectly Affected):

- 🔒 RBAC/ABAC prevents unauthorized access to crew data
- ⚠ If authenticated user's account compromised, crew data at risk
- 📋 Can request "Who accessed my data?" (requires expanded audit logging)

---

6. US 3.6.2 Compliance - Personal Data Breach Handling

6.1. What Constitutes a Personal Data Breach

GDPR Definition (Article 4(12)):

A breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data.

Three Types:

1. **Confidentiality Breach:** Unauthorized access or disclosure
   - Example: JWT token stolen via XSS, attacker accesses VVN data
2. **Integrity Breach:** Unauthorized alteration
   - Example: SQL injection changes crew CitizenId values
3. **Availability Breach:** Loss or destruction
   - Example: Database server crash, corrupted backups

6.2. Sprint B Breach Scenarios

Scenario 1: JWT Token Theft via XSS

Classification: Confidentiality breach

Data Affected:

- Primary: Admin's credentials (email, name, userId)
- Secondary: All data accessible to Admin role (500+ crew records)

Risk to Individuals: HIGH (admin has access to sensitive crew CitizenId)

Notification Required: ☑ YES (Article 33 - within 72 hours)

Scenario 2: Activation Email Sent to Wrong Address

Classification: Confidentiality breach

Data Affected: Intended user's email, name, activation token

Risk to Individuals: LOW-MEDIUM (wrong recipient knows someone is being onboarded)

Notification Required: ⚠ MAYBE (assess risk level)

Scenario 3: Google OAuth Account Takeover

Classification: Confidentiality breach + possible integrity breach

Data Affected: All data accessible to victim's role

Risk to Individuals: HIGH (especially if PortAuthorityOfficer - access to all crew data)

Notification Required: ☑ YES (Article 33)

Special Note: System is data controller and remains responsible even if third-party IAM compromised

---

6.3. Notification to Supervisory Authority (Article 33)

When to Notify:

Mandatory: Within 72 hours of becoming aware of breach

Exemption: Unless breach unlikely to result in risk to individuals' rights and freedoms

Risk Assessment Criteria:

- Type of data: Crew CitizenId (high risk) vs. organization name (low risk)
- Volume: Single user (low) vs. database dump (high)
- Ease of identification: Direct identifiers (high risk)
- Severity: Financial loss, identity theft, discrimination

Required Information (Article 33(3)):

1. **Nature of Breach:**
    - What happened?
    - Date and time of breach
    - Categories of data subjects affected
    - Categories of personal data affected
2. **Contact Point:**
    - Data Protection Officer (DPO) name and contact
3. **Likely Consequences:**
    - What harm could result?
    - How many individuals affected?
4. **Measures Taken:**
    - Immediate actions (revoked tokens, disabled accounts)
    - Mitigation (forced re-authentication, implemented CSP)
    - Prevention (reduced token lifetime, added MFA)

6.4. Notification to Data Subjects (Article 34)

When to Notify:

When breach **likely to result in high risk** to individuals' rights and freedoms

Exemptions:

1. Data was encrypted or unintelligible
2. Subsequent measures ensure high risk no longer likely
3. Disproportionate effort → Public communication instead

High Risk Indicators:

- Sensitive data exposed (CitizenId, health, financial)
- Large volume affected
- Severe consequences (identity theft, discrimination)

Required Information (Article 34(2)):

1. Nature of breach (clear, plain language - no jargon)
2. Contact point (DPO)
3. Likely consequences
4. Measures taken and actions data subjects should take

6.5. Deadline for Breach Notification

Supervisory Authority (Article 33):

- **Deadline:** 72 hours after becoming aware
- **"Becoming Aware":** Reasonable certainty that breach occurred (not first suspicion)

Example Timeline:

```
09:45 - Breach occurs
10:30 - Security alert triggered
10:35 - Investigation confirms breach ← "BECOMING AWARE" starts
16:00 - Notification submitted (6 hours - compliant)
```

If Deadline Missed: Notification still required + explain delay

---

Data Subjects (Article 34):

- **Deadline:** "Without undue delay" (no specific timeframe)
- **Interpretation:** Days, not weeks

Urgency Factors:

- Can subjects take action to mitigate? → Notify faster
- High severity? → Notify faster
- Large volume? → May need more prep time

Typical Timelines:

- High risk + urgent action: 1-2 days
- High risk + no immediate action: 3-5 days
- Medium risk: 7-14 days

---

7. Future Problems and Required Improvements

7.1. Critical Gaps

Gap 1: No Encryption at Rest for CitizenId

- **Risk:** Database breach exposes 500+ crew/representative national IDs
- **GDPR Violation:** Article 32 (Security of Processing)
- **Mitigation:** Implement column-level encryption (AES-256) or Transparent Data Encryption (TDE)

Gap 2: No Data Retention Policy

- **Risk:** Personal data retained indefinitely
- **GDPR Violation:** Article 5(1)(e) (Storage Limitation)
- **Mitigation:**
  - Crew data: Delete 90 days after vessel departure
  - Inactive users: Anonymize after 2 years
  - Audit logs: Archive after 5 years

Gap 3: XSS-Vulnerable Token Storage

- **Risk:** Malicious script can steal JWT from localStorage
- **GDPR Violation:** Article 32 (inadequate security)
- **Mitigation:** Store refresh tokens in httpOnly cookies

Gap 4: No Data Processing Agreements with Google

- **Risk:** Non-compliance with processor requirements
- **GDPR Violation:** Article 28(3) (processor obligations)
- **Mitigation:** Establish DPA for Google OAuth and Gmail SMTP

7.2. High Priority Improvements

Gap 5: No Subject Access Request (SAR) Mechanism

- **Risk:** Cannot fulfill Article 15 (Right of Access) requests
- **Mitigation:** Implement API endpoint to export user's data in JSON/XML

Gap 6: Incomplete Audit Logging

- **Risk:** Cannot detect unauthorized access or provide access history
- **Mitigation:** Log all authentication events, API access, authorization failures

Gap 7: No Token Revocation Mechanism

- **Risk:** Compromised tokens remain valid until expiration
- **Mitigation:** Implement token revocation list (Redis), reduce token lifetime

Gap 8: No Privacy Policy

- **Risk:** Users not informed about data processing
- **GDPR Violation:** Article 13 (Information to be provided)
- **Mitigation:** Create comprehensive privacy policy, display during authentication

---

7.3. Medium Priority Improvements

Gap 9: No Data Portability

- **Risk:** Cannot fulfill Article 20 (Right to Data Portability)
- **Mitigation:** Export functionality for user data in machine-readable format

Gap 10: No Breach Detection and Notification System

- **Risk:** Cannot comply with 72-hour notification requirement
- **Mitigation:** Security monitoring, alerting, breach response procedures

Gap 11: No Right to Erasure Implementation

- **Risk:** Cannot fulfill Article 17 (Right to be Forgotten)
- **Mitigation:** Hard delete capability + anonymization procedures

Gap 12: Activation Token Security

- **Risk:** Tokens not cryptographically signed, no rate limiting
- **Mitigation:** Sign tokens, implement rate limiting, reduce expiration to 24 hours

---

8. Regulatory Framework for Port Operations

8.1. 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 (Article 6(1)(c) - Legal Obligation)
- Mandates retention of vessel visit records for security purposes
- Potential conflict with GDPR storage limitation → Legal obligation overrides

EU Regulation 725/2004 (Maritime Security):

- Implements ISPS Code in EU law
- Justifies crew data processing for customs clearance

- May require longer retention than GDPR preference

8.2. 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)
- No separate consent required

Law Enforcement Requests:

- Police/customs may request crew data for investigations
- Article 23 GDPR allows restrictions on data subject rights
- Must log all disclosures

8.3. Joint Controllers and B2B Processing

Shipping Agents as Joint Controllers:

- Both Port Authority and Shipping Agents determine purposes/means
- Requires Joint Controller Agreement (Article 26)
- Must define responsibilities for SARs, breach notification, data retention

Current Gap: No Joint Controller Agreement in place

---

9. Recommended GDPR Compliance Roadmap

Phase 1: Foundation (Months 1-3)

Immediate Actions:

1. Encrypt sensitive data (CitizenId, TaxNumber) - Column-level encryption
2. Migrate refresh tokens to httpOnly cookies (fix XSS vulnerability)
3. Reduce access token lifetime to 15 minutes
4. Implement Content Security Policy (CSP) headers
5. Establish Data Processing Agreements with Google (OAuth + Gmail SMTP)

Short-Term Actions: 6. Create and publish Privacy Policy 7. Implement data access audit logging (authentication, API access, authorization failures) 8. Organizational data isolation verification (ensure ShippingAgentRep cannot access other orgs) 9. Activation token security improvements (reduce expiration, rate limiting, cryptographic signing)

Phase 2: Core Compliance (Months 4-6)

10. Deploy data retention policy with automated purging
11. Implement Subject Access Request (SAR) API endpoint
12. Token revocation mechanism (Redis-based)

13. Draft Joint Controller Agreements with shipping agents
14. Establish breach detection and notification procedures
15. Expand audit logging to include data access events

Phase 3: Advanced Features (Months 7-12)

16. Implement Right to Erasure (hard delete + anonymization)
17. Data Portability API (export in machine-readable format)
18. Conduct Data Protection Impact Assessment (DPIA) for high-risk processing
19. Device fingerprinting for anomaly detection
20. Multi-factor authentication (MFA) for sensitive actions
21. Behavioral analytics for unauthorized access detection

Phase 4: Continuous Improvement (Ongoing)

22. Quarterly GDPR compliance audits
23. Staff training on data protection principles
24. Monitor EDPB guidance and ECJ rulings for updates
25. Privacy-by-design reviews for all new features
26. Regular penetration testing and security assessments

---

10. Conclusion

10.1. Current State of the Project

The Port Management System has made significant progress in Sprint B with the introduction of secure authentication via Google OAuth and role-based access control. These additions improve security by eliminating password storage and enforcing organizational data isolation. However, critical GDPR compliance gaps remain that must be addressed before the system can be considered production-ready.

Key Achievements:

- ☑ External authentication via Google OAuth reduces password-related risks
- ☑ RBAC/ABAC implementation prevents unauthorized data access
- ☑ Organizational data isolation protects commercial confidentiality
- ☑ Basic audit logging for VVN approval decisions

Critical Gaps:

- ❌ No encryption at rest for sensitive data (crew/representative CitizenId)
- ❌ No data retention policy (indefinite storage violates Article 5(1)(e))
- ❌ XSS-vulnerable token storage (localStorage)
- ❌ No Data Processing Agreements with Google services
- ❌ No Subject Access Request mechanism (Article 15)
- ❌ No breach notification procedures (Article 33/34)
- ❌ Incomplete audit logging (cannot track data access)

10.2. Most Important GDPR Considerations

Priority 1: Protect Highly Sensitive Data (CitizenId)

Crew members and representatives' national identification numbers are **special category data** under GDPR. Database compromise would expose 500+ individuals to identity theft risk. Encryption at rest is not optional - it is explicitly required by Article 32 (Security of Processing).

Action: Implement column-level encryption (AES-256) or database-level Transparent Data Encryption.

Priority 2: Establish Legal Framework with Third Parties

Google acts as data processor for both authentication (OAuth) and email delivery (Gmail SMTP). Without formal Data Processing Agreements (Article 28), the system operates in legal limbo. If Google experiences a data breach affecting Port Management System users, lack of DPA could result in supervisory authority sanctions.

Action: Establish DPAs with Google within 1 month. Consider migrating to EU-based email service provider with clear GDPR compliance.

Priority 3: Implement Data Retention and Deletion

Personal data is currently retained indefinitely. This violates the storage limitation principle (Article 5(1)(e)) and prevents fulfillment of erasure requests (Article 17). Maritime regulations (ISPS Code) may require retention of security-related records, but operational data should have defined retention periods.

Action:

- Define retention policy: Crew data (90 days post-departure), inactive users (2 years), audit logs (5 years)
- Implement automated purging jobs within 2-3 months
- Create hard delete capability for erasure requests

Priority 4: Fix Token Storage Vulnerability

Storing JWT tokens in browser localStorage creates XSS vulnerability. A single successful script injection could compromise multiple user sessions. Given that admin accounts have access to all crew CitizenId data, this represents a **high-risk data breach scenario**.

Action: Migrate refresh tokens to httpOnly cookies (straightforward implementation).

Priority 5: Establish Breach Response Procedures

Article 33 requires notification to supervisory authority within 72 hours of becoming aware of a breach. Without documented procedures, the organization cannot meet this deadline. Several Sprint B breach scenarios (token theft, OAuth compromise, email interception) are realistic threats.

Action:

- Document breach detection, assessment, and notification procedures within 1 month

- Implement security monitoring and alerting
- Train team on breach response protocol
- Create notification templates for supervisory authority and data subjects

10.3. Critical Mitigations Summary

Risk	Priority	Mitigation	Timeline	GDPR Articles
CitizenId exposure	◍ Critical	Encrypt at rest (AES-256)	1-2 months	Art. 32
Indefinite data retention	◍ Critical	Retention policy + automated purging	2-3 months	Art. 5(1)(e), 17
XSS token theft	◍ Critical	httpOnly cookies, CSP headers	1-2 weeks	Art. 32
No DPA with Google	◍ High	Establish formal DPAs	1 month	Art. 28
No SAR mechanism	◍ High	Implement data export API	2-3 months	Art. 15
No breach procedures	◍ High	Document + train team	1 month	Art. 33, 34
Incomplete audit logs	◍ Medium	Log authentication, access, failures	1-2 months	Art. 30
No privacy policy	◍ Medium	Create and publish policy	2-4 weeks	Art. 13
Token not revocable	◍ Medium	Redis revocation list	1 month	Art. 32
Activation token security	◍ Medium	Sign tokens, rate limit, reduce expiry	2-3 weeks	Art. 32

10.4. Final Recommendations

For Production Deployment:

The system cannot be deployed to production without addressing the four critical risks (CitizenId encryption, data retention policy, token storage vulnerability, DPAs with Google). These represent fundamental GDPR violations that expose the organization to:

- Supervisory authority fines (up to €20 million or 4% of annual global turnover)
- Data subject litigation
- Reputational damage
- Operational shutdown orders

Recommended Approach:

1. **Immediate (Next 2 Weeks):** Fix token storage (httpOnly cookies), implement CSP headers, reduce token lifetime
2. **Month 1:** Establish DPAs with Google, create privacy policy, document breach procedures
3. **Months 2-3:** Implement encryption at rest, deploy data retention policy with automated purging
4. **Months 3-6:** SAR mechanism, token revocation, expanded audit logging, Joint Controller Agreements
5. **Months 6-12:** Data portability, DPIA, MFA, behavioral analytics

Estimated Compliance Timeline: 6 months for core compliance, 12 months for full GDPR maturity

Estimated Effort: 2-3 full-time developers + 1 data protection advisor

---

11. References

11.1. GDPR and Data Protection Framework

1. **Regulation (EU) 2016/679 (GDPR)**
European Parliament and Council. (2016). *General Data Protection Regulation*.
Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj

2. **European Data Protection Board (EDPB)**
EDPB. (2025). *Guidelines and Recommendations on GDPR Compliance*.
Available at: https://edpb.europa.eu/our-work-tools/general-guidance_en

3. **Portuguese Supervisory Authority (CNPD)**
Comissão Nacional de Proteção de Dados. (2025). *Data Protection Authority Portal*.
Available at: https://www.cnpd.pt/

4. **EDPB Guidelines 4/2019 on Article 25**
European Data Protection Board. (2020). *Guidelines on Data Protection by Design and by Default*.
Available at: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en

5. **EDPB Guidelines 07/2020 on Controller-Processor Relationship**
European Data Protection Board. (2021). *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*.
Available at: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en

11.2. International Data Transfers

6. **EU-US Data Privacy Framework**
European Commission. (2023). *Adequacy Decision for the EU-US Data Privacy Framework*.
Available at: https://www.dataprivacyframework.gov/

7. **Standard Contractual Clauses (SCCs)**
European Commission. (2021). *Implementing Decision on standard contractual clauses for international data transfers*.
Available at: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

8. **EDPB Recommendations 01/2020 on Schrems II**
European Data Protection Board. (2020). *Recommendations 01/2020 on measures that supplement transfer tools*.
Available at: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en

11.3. Maritime and Port Security Regulations

9. **International Ship and Port Facility Security (ISPS) Code**
International Maritime Organization (IMO). (2003). *ISPS Code - Part A and Part B*.
Available at: https://www.imo.org/en/OurWork/Security/Pages/SOLAS-XI2%20ISPS%20Code.aspx

10. **EU Regulation 725/2004**
European Parliament and Council. (2004). *Regulation on enhancing ship and port facility security*.
Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32004R0725

11. **IMO FAL Convention**
International Maritime Organization. (1965, amended 2022). *Convention on Facilitation of International Maritime Traffic*.
Available at: https://www.imo.org/en/About/Conventions/Pages/Convention-on-Facilitation-of-International-Maritime-Traffic-(FAL).aspx

11.4. Third-Party Service Providers

12. **Google Privacy Policy**
Google LLC. (2025). *Privacy Policy*.
Available at: https://policies.google.com/privacy

13. **Google OAuth 2.0 Documentation**
Google Identity Platform. (2025). *Using OAuth 2.0 to Access Google APIs*.
Available at: https://developers.google.com/identity/protocols/oauth2

14. **Google Cloud Data Processing Terms**
Google Cloud. (2025). *Data Processing and Security Terms*.
Available at: https://cloud.google.com/terms/data-processing-terms

11.5. Security Standards and Best Practices

15. **OWASP Top 10 Web Application Security Risks**
OWASP Foundation. (2021). *OWASP Top 10:2021*.
Available at: https://owasp.org/www-project-top-ten/

16. **NIST Cybersecurity Framework**
National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity*.
Available at: https://www.nist.gov/cyberframework

17. **ISO/IEC 27001:2022**
International Organization for Standardization. (2022). *Information security management systems -*

Requirements.
Available at: https://www.iso.org/standard/27001

11.6. Technical Documentation

18. **JWT (JSON Web Token) Specification - RFC 7519**
Internet Engineering Task Force (IETF). (2015). *JSON Web Token (JWT)*.
Available at: https://datatracker.ietf.org/doc/html/rfc7519

19. **OAuth 2.0 Authorization Framework - RFC 6749**
Internet Engineering Task Force (IETF). (2012). *The OAuth 2.0 Authorization Framework*.
Available at: https://datatracker.ietf.org/doc/html/rfc6749

20. **Content Security Policy (CSP) Level 3**
W3C. (2024). *Content Security Policy Level 3 - W3C Working Draft*.
Available at: https://www.w3.org/TR/CSP3/