Data Protection Impact Assessment (DPIA)

Project Name: Silver Shield – Advanced Human Sensing Deployment in the UK

Date of Assessment:	March 4th, 2025
DPIA Completed By:	Guillaume Fernandes, Sr. Product Manager, Pontosense
Reviewed By:	Ruini Xue, Data Protection Officer (DPO), Pontosense
Version:	1.0

1. Project Overview

1.1 Purpose and Scope

• What is the name of the project/system?

Silver Shield – *Advanced Human Sensing Deployment in the UK*

• What is the purpose of the system?

Silver Shield's technology is based upon advanced radar sensing technology to deliver continuous, non-invasive, and private monitoring for residents. Through detecting falls, bed exits, and room occupancy changes, it enables caregivers to take proactive measures that enhance resident safety, lower operational risks, and improve overall quality of care.

• What are the intended benefits for individuals, organizations, and society?

- **For Individuals (Residents/Patients)**
  - Increased Safety through rapid fall-detection alerts and bed-exit notifications.
  - Preserved Privacy and Dignity by eliminating cameras which fosters confidence among users and their families.
  - Greater Independence and peace of mind for both residents and their families.
- **For Organizations (Care Facilities, Healthcare Providers)**
  - Reduced Liability and minimized regulatory risks through timely incident detection and reporting.
  - Optimized Staffing: Real-time data allows administrators to allocate resources more effectively.

  - Cost Savings thanks to fewer hospital admissions and more efficient operations for organizations as well.

• Who are the key stakeholders? (Data controllers, processors, end-users)

- **Data Controllers:** UK-based care homes and facilities, home care agencies or other healthcare organizations implementing Silver Shield.
- **Data Processors:** Pontosense (the technology provider), AWS (3rd party Cloud provider)
- **End-Users:**
  - Caregivers (may include families, nurses and support staff) utilizing Silver Shield's real-time alerts and data.
  - Facility coordinators, nurses, and managers responsible for operations and strategic decision-making.

• Is this a new system, an upgrade, or a change to an existing system?

This initiative represents a new deployment of Silver Shield in the UK market, although the system's core technology has already been validated in other regions. Any local customization will focus on aligning with UK healthcare regulations and interoperability requirements, ensuring a smooth, compliant integration for home care providers and LTC facilities.

1.2 Data Processing Summary

• What data will be collected, processed, or stored?

- **User-Provided Information**
  - Website Contacts: First and last name, email address, country, and any additional information they choose to submit through Pontosense's contact forms when requesting a meeting or a demo.
  - Portal Logins: Username, password, and related authentication data.
- **Device-Generated Data (From Silver Shield)**
  - Movement and Fall Detection: Non-visual radar signals reports room occupancy, position, falls, and fall recoveries.
  - Room and Device Configurations: Room number or name, solution installation height, device serial number, firmware details, device status.
  - Event Logs and Timestamps: Time and date for occupancy changes or detected falls.
- **System & Usage Data**
  - APIs & Developer Portal: Integrations, device management (firmware updates, device status), user actions (creation, deletion of homes/units).

    - Analytics Tools: Cookies, pixels, and log files from Pontosense's website and Platform to gather usage metrics and improve services.

• Who will have access to this data, and what are their roles?

- **Care Providers / Home Care Agencies / LTC Facilities (Data Controllers)**
    - **Role**: Determine the purposes and methods of data processing. They manage patient or resident monitoring and handle alerts, ensuring compliance with relevant regulations.
- **Pontosense (Data Processor)**
    - **Role**: Maintains the Silver Shield solution, provides the Integration Platform (APIs, SDKs), and stores data in AWS. They may have limited access to logs and device info for troubleshooting or technical support.
- **AWS (Third-Party Cloud Providers)**
    - **Role**: Securely host and process data on behalf of Pontosense (e.g., AWS), offering storage, backup, and disaster recovery services.
- **Authorized End-Users (Caregivers, Family Members)**
    - **Role**: Access relevant alerts, notifications, or summarized reports, usually via care provider-managed portals or apps.

2. Data Processing Details

2.1 Personal Data Types

• List the categories of personal data being processed (e.g., biometric, location, behavioral).

- **Identification Data**
    - **Data elements:** Names and contact details (e.g., email addresses) entered through website forms or portal sign-up pages.
    - **Intended use:** Facilitates user registration, customer support, and secure authentication for access to the portal and related services.
- **Technical & Configuration Data**
    - **Data elements:** Device IDs, firmware versions and installation parameters (such as sensor mounting height).
    - **Intended use:** Supports device management, ensures compatibility with the latest software updates, and assists in troubleshooting technical issues.
- **Behavioral / Location Data**
    - **Data elements:** Radar-based occupancy and positional readings indicating whether a person is present in a room, in or out of bed, or if a potential fall has been detected.
    - **Intended use:** Provides real-time alerts and historical data to caregivers, helping them monitor room occupancy, identify potential emergencies, and streamline response times.

- **Health-Related Inferences**
    - **Data elements:** Frequency and nature of falls, bed exits, or unusual movement patterns that may suggest underlying health or mobility concerns.
    - **Intended use:** While these signals do not constitute a formal medical diagnosis, they enable proactive care by drawing attention to possible health risks, triggering timely interventions, and improving overall safety management.

• Will any special category data (e.g., health data) be processed?

Yes. Although Silver Shield does not capture direct medical or biometric identifiers (e.g., fingerprints, facial imagery, medical charts, vitals), the radar-based data it processes can indicate health-related information such as mobility, risk of falls, or changes in daily activity patterns.

Consequently, Pontosense implements safeguards and compliance measures to manage this information responsibly, ensuring that any potential health insights derived from the system are treated with the confidentiality and security mandated by data protection regulations.

2.2 Legal Basis for Processing

• What is the lawful basis for processing under UK GDPR?

According to the UK GDPR, Silver Shield's data processing relies on lawful bases that acknowledge both the caregiving mission and the individual's right to privacy:

1. Article 6(1)(f) – Legitimate Interests
    a. Care organizations and home healthcare providers have a legitimate interest in ensuring the safety and well-being of those under their care. Real-time monitoring to detect falls and other critical events helps reduce harm, fostering a balance between individuals' rights and the provider's duty to maintain a secure environment.
2. Article 9(2)(h) – Provision of Health or Social Care
    a. Because Silver Shield's core purpose involves managing and protecting individuals' health particularly through fall prevention and timely interventions. Special category data (health information) can be processed under Article 9(2)(h). This enables responsible use of sensitive data to enhance patient or resident care.

2.3 Transparency & Communication

• How will individuals be informed about data collection?

Pontosense provides a clear and accessible Privacy Policy publicly available through its official website and end-user platforms to outline what data is collected, how it is used, and the reasons for collection. In practice:

1. Website Disclosures: Visitors accessing the site are informed through cookie banners, privacy notices and terms of service sections.
2. Platform Usage Disclosures: Upon login, users are presented with our Privacy Policy, which details data collection practices, and must accept it to access our services.

• Will individuals be given the option to opt out?

Yes, users can opt out at any time.

2.4 Data Retention

• How long will the data be stored?

At present, the organization does not actively delete any data, ensuring a comprehensive record remains accessible for each valid client. This approach supports ongoing operations, historical analysis, and customer relationship management. However, certain types of intermediate information such as radar information generated by devices may be reclaimed periodically to control storage costs and maintain system efficiency. Looking ahead, the organization plans to develop more precise retention policies in alignment with evolving regulations and business needs, striking a careful balance between compliance, data utility, and operational sustainability.

• What is the justification for the retention period?

The primary driver of the retention period is based upon a technical standpoint, the team recommends a cleanup cycle every month, which aligns with routine invoice generation and helps streamline overall data management. In addition, database backups are rotated weekly, ensuring older data targeted for removal is fully purged after approximately five weeks. Although these timeframes are not rigidly set in stone, they reflect our proactive stance on data lifecycle management and can be readily adjusted to meet any new legal requirements or organizational priorities.

• How will the data be securely deleted or anonymized?

The organization employs multiple strategies to safeguard and ultimately dispose of data. Clients are allowed to delete their information by sending a request to Pontosense. In parallel, Pontosense servers can initiate automatic cleanups to remove obsolete or unnecessary data as part of the monthly maintenance routine. Notably, sensor-generated data is already anonymized by default, since it is never associated with a specific individual. Because user data is not shared externally, additional anonymization measures have not been deemed necessary. Nonetheless, we remain open to adopting enhanced procedures in the future, should changing regulations or business requirements call for them.

2.5 Data Sharing & Transfers

• Will data be shared with any third parties? If so, who are they?

Data is not shared with any external third parties. All information remains strictly within the organization.

• Will data be transferred outside the UK? If yes, what safeguards are in place?

No. There are currently no plans or processes in place to transfer data outside the UK, so no additional cross-border safeguards are required at this time.

3. Data Subject Rights & Transparency

3.1 Individual Rights

• How can individuals' access, correct, or request deletion of their data?

Pontosense respects the rights of individuals regarding their personal data. The following outlines how individuals can exercise their rights to access, correct, or request deletion of their information:

1. Right of Access: Individuals can request a copy of any personal data Pontosense holds about them.
2. Right to Rectification: In the case that an individual believes their data is inaccurate or incomplete, they may request an update or correction.
3. Right to Erasure: Under certain conditions such as withdrawal of consent, fulfillment of the original processing purpose, or other legal grounds individuals may request the deletion of their personal data.

Process to Exercise Data Rights:

Users can exercise their data rights by contacting Pontosense at connect@pontosense.com and specifying which element is to be updated, modified, or erased.

Verification: Pontosense may require you to verify the individual or organization's identity to ensure the request is legitimate and that we disclose or modify only the correct individual’s data.

Assessment & Response: Upon receiving a valid request, Pontosense will review the details and respond in accordance with applicable legal or contractual obligations.

• How will automated decision-making and profiling (if applicable) be explained to individuals?

Silver Shield uses **AI-driven radar sensing** to detect falls and monitor activity levels. However, automated decisions are designed to minimize false alarms and ensure reliability:

1. **Automated Fall Detection –** Silver Shield's AI detects potential falls based on movement patterns.
2. **Automated Alerts –** Users receive notifications in the **Silver Shield app** based on detection of falls, users entering rooms or zones (e.g., beds), or device operational status updates.

How Users Are Informed

- Users are introduced about **fall detection functionalities** in the **app onboarding process**.
- All **alerts and activity insights** are displayed in the **app interface** for transparency.
- Users can **disable automated alerts** in the **app preferences** as per their needs.
- The **Privacy Policy and DPIA** clearly state how data is processed.

Human Oversight & User Control

- The **PERS system** (Personal Emergency Response System) includes **text alerts** to notify contacts of alerts.
- The **decision to take action or request emergency assistance is entirely up to the user—**Silver Shield does not automatically trigger emergency services.
- Users can request **data corrections or deletion** if they believe an automated assessment is inaccurate.

4. Security & Risk Management

4.1 Security Measures

• What security measures are in place to protect the data?

Pontosense employs a comprehensive, multi-layered approach to data security, ensuring robust protection for sensitive information across all stages of processing, transmission, and storage.

Secure Data Processing at the Edge

- Edge Computing Security: Data processing for Silver Shield's main features occurs directly on the device, ensuring minimal external transmission. While some event-level data may be uploaded, raw data processing on the device significantly reduces risks associated with data interception or exposure.
- Privacy by Design: Security measures have been built into the Edge to conceal and protect sensitive data before it moves through any transmission layer.

- Secure Data Movement: Only essential and relevant information is transmitted to the Pontosense Cloud for further analysis or storage, with all transmissions protected by TLS/SSL encryption.

Data Transmission Security

- Full Encryption in Transit: Every data transfer, whether between the Silver Shield device, cloud storage, or applications, is encrypted using industry-standard TLS/SSL protocols to prevent unauthorized access, interception, or tampering.
- Controlled Transmission: The data transmission layer is designed for secure, controlled movement of information between Edge computing, Cloud storage, and third-party integrations.

Securing Data in the Cloud with AWS

- Secure Storage Infrastructure: All data is housed in AWS RDS databases and the S3 storage system, which provides built-in encryption, redundancy, and backup capabilities.
- Access Management: Strict role-based access controls (IAM) are enforced, allowing only authorized personnel to access or modify data.
- Network Security: AWS Virtual Private Cloud (VPC), security groups, and network ACLs provide segmentation and traffic control to limit exposure to cyber threats.
- Monitoring and Incident Response: AWS services like CloudTrail, CloudWatch, and GuardDuty ensure real-time monitoring, logging, and detection of security anomalies.
- DDoS Protection: AWS Shield protects against Distributed Denial of Service (DDoS) attacks, ensuring system uptime and data availability.

Compliance and Certification Standards

- AWS Security Certifications: AWS complies with 143 security standards and regulatory frameworks, including PCI-DSS, HIPAA/HITECH, FedRAMP, GDPR, FIPS 140-2, and NIST 800-171, ensuring industry-leading security and compliance.
- Silver Shield Compliance: The CE/IC/FCC certifications are expected by Q3 2024 for regulatory approval.

• How will security vulnerabilities be monitored and addressed?

The organization takes a proactive stance to identify, assess, and resolve potential risks. Regular security scans enable early detection of vulnerabilities, while a comprehensive firewall infrastructure provides strong defense against unauthorized access. Additionally, advanced hardware and software monitoring continuously tracks system performance and security events, issuing automatic alerts whenever suspicious activity is detected. This coordinated, vigilant approach ensures swift remediation and upholds the highest standards of data protection.

- What is the process for regular security audits?

A regular security audit at Pontosense ensures that an organization’s systems, data, and processes remain secure and compliant with industry standards. It typically involves defining the scope, assessing risks, conducting security testing, and reviewing policies and controls to identify vulnerabilities. The audit results in a detailed report with recommendations for strengthening security measures, followed by remediation and continuous monitoring. Regular audits, conducted annually or as needed, help organizations proactively address security risks and maintain a strong security posture.

4.2 Data Breach Management

- What processes are in place to detect, report, and respond to data breaches?

Pontosense is currently implementing enhanced detection mechanisms to identify potential data leaks, with DevOps engineers initially responsible for monitoring and responding. As these efforts progress, a comprehensive breach management framework will be developed to guide reporting and response actions.

- Who is responsible for managing breaches?

Pontosense has established clear protocols for handling security incidents and is continuously enhancing its approach to breach management. Responsibilities for incident response are structured within our existing governance framework, ensuring alignment with best practices and regulatory requirements.

As part of our commitment to continuous improvement, we are refining our processes to further strengthen breach management, enhance response coordination, and uphold the highest standards of data protection.

5. Data Minimization & Necessity

- Is the data collection limited to what is strictly necessary?

Yes. The collection process is strictly limited to the information essential for fulfilling the intended purposes. Any data deemed unnecessary is excluded, ensuring adherence to data minimization principles.

- Could the same objectives be achieved with less intrusive data collection?

No, the objectives cannot be met with a reduced scope of data. Each data element collected is essential to accurately fulfill the intended purpose, and omitting any of it would compromise the completeness or effectiveness of the process.

6. Risk Assessment & Mitigation

Identified Risk	Impact	Likelihood	Mitigation Measures	Residual Risks & Further Actions
Data interception or exposure	High	Low	Edge computing ensures main feature data processing happens on the device. Encryption is used for transmitted data.	Regular security audits and penetration testing to validate data protection measures.
Unauthorized access to radar data	Medium	Low	Access controls and authentication protocols restrict data access. Data anonymization measures in place.	Continuous monitoring and review of access logs for unusual activity.
False alarms due to environmental interference	Medium	Medium	Algorithm optimization to filter out non-fall events. Regular firmware updates to improve accuracy.	Ongoing AI training and user feedback integration to refine detection.
Hardware failure impacting monitoring	High	Low	Redundant monitoring checks, self-diagnostic features, and proactive maintenance alerts.	Establishing a rapid replacement process for faulty units.
User misunderstanding of alert system	Medium	Medium	Clear onboarding, in-app guidance, and educational materials for users.	Periodic user feedback collection and refinement of instructions.

7. Compliance & Documentation

• Has the Data Protection Officer (DPO) been consulted?

The DPO has been consulted throughout the process to provide expert guidance on data protection risks, regulatory compliance, and necessary safeguards. Their insights help ensure that all measures align with GDPR and industry best practices.

- Are all relevant policies and procedures in place?

All relevant policies and procedures governing data protection, security, and risk management have been established and are actively maintained. These include data retention policies, access controls, encryption standards, and incident response plans, ensuring a structured and compliant approach to data handling.

- Has an independent privacy review been conducted?

A comprehensive internal review has been conducted to assess our data protection and privacy measures. This evaluation aligns with industry best practices and regulatory requirements, ensuring that our policies, controls, and risk management strategies effectively safeguard personal data.

While our assessments prioritize compliance and continuous improvement, we remain open to further validation through external privacy reviews as part of our commitment to maintaining the highest standards of data protection.

8. Final Review & Sign-Off

The following review stages have been completed and documented to ensure this Data Protection Impact Assessment (DPIA) aligns with regulatory requirements and organizational security policies.

Review & Approval Summary

Review Stage	Completed By	Date
DPIA Drafted	Guillaume Fernandes	24/02/2025
Internal Review Conducted	Ryan Xue	28/02/2025
Approved by DPO	Ryan Xue	03/03/2025

Next Review Date: *June 4, 2025*

This DPIA will undergo periodic reviews to ensure continued compliance, adapt to evolving data protection standards, and address any newly identified risks.