# DPIA for AmbuDispatch

## Step 1: Identify the need for a DPIA

| Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA. |
| --- |
| This project aims to create a web-based application for Saint John Ambulance, designed to streamline the dispatch and management of resources at incidents. It seeks to address shortcomings in existing Dispatch systems by introducing key functionalities such as priortising calls, resource assignment, and maintaining a control room log. The initiative is driven by the need to improve operational efficiency and enhance user accessibility, with additional features like a user-friendly interface, real-time location tracking and improved break management.<br><br>The processing activities will involve the collection, storage and management of personal data related to both the individuals in need of medical assistance e.g., ASHICE reports containing Age, Sex, History, Injuries, Condition, everything else) and the personnel involved in providing that assistance. The application will facilitate real-time communication and dispatching decisions, aiming to minimise response times and improve patient care.<br><br>The need for a DPIA was identified due to the project's extensive processing of personal data, which includes sensitive health information and real-time location data of both patients and ambulance crew members. Given the application's critical role in emergency health services and its potential to significantly impact the rights and freedoms of individuals, conducting a DPIA is essential to ensure compliance with data protection regulations, notably the GDPR. The DPIA will help identify and mitigate any risks related to privacy, data protection, and individual rights, ensuring that the project incorporates data protection by design and by default. |

# Step 2: Describe the processing

| **Describe the nature of the processing:** how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved? |
| --- |
| Data will be collected directly from multiple sources, including inputs from control room staff and the ambulance crew on the ground. Information collected includes ASHICE reports (Age, Sex, History, Injuries, Condition, Everything else) for patients and operational data for resources (e.g., location, status, and break times).<br>The data will be used to dispatch resources efficiently, manage calls and priorities, maintain a control room log, and enable real-time decision-making. Enhanced features such as a live map view and break management are designed to improve response times and overall operational efficiency.<br>Data will be securely stored on servers managed by the University of Birmingham (UoB), with robust encryption and access control mechanisms in place. These storage solutions are designed to be fully compliant with GDPR standards, safeguarding data from unauthorised access and potential breaches.<br>Data will be retained only for as long as necessary for the purposes for which it was collected, in line with legal requirements and Saint John Ambulance policies. An automated process will delete data no longer needed, and users can manually delete data where appropriate.<br>Data sharing will be strictly controlled and limited to necessary instances, such as with healthcare providers or emergency services, under compliant data sharing agreements. Any sharing will be documented and conducted in line with GDPR principles.<br>The processing activities within the Saint John Ambulance web application involve handling sensitive health-related information and real-time location data, which are considered high-risk due to the necessity for strict security and privacy controls. The application's capacity for real-time decision-making, which is crucial for health outcomes, emphasizes the need for reliable, accurate, and timely processing of data. Moreover, the inherent sensitivity of the data elevates the risk of breaches, underscoring the importance of implementing comprehensive cybersecurity measures to protect against such incidents. |

| **Describe the scope of the processing:** what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover? |
| --- |
| The data encompasses both general personal data (e.g., names and contact information of ambulance crew and other staff) and special category data under GDPR, notably health-related information from ASHICE reports (Age, Sex, History, Injuries, Condition, Everything else), as well as real-time location data of patients and ambulance crew. No criminal offence data is intended to be processed by this application. The volume of data collected will vary depending on the number of incidents covered by Saint John Ambulance and the scale of these incidents. Data collection and usage will occur in real-time, with every call or dispatch action generating new data. The system is designed to handle multiple incidents simultaneously, indicating a substantial and continuous flow of data. Data will be kept only as long as necessary for the purpose for which it was collected, in compliance with legal requirements and organisational policies. This period will vary by data type for example, operational data may be kept for shorter periods than medical records, which may be subject to specific regulatory retention requirements. The individuals affected include patients requiring medical assistance at incidents, ambulance crew members, and other operational staff. The number of affected individuals will fluctuate based on the incident size and frequency but could potentially encompass thousands of individuals annually. The processing will be confined to the operational region of Saint John Ambulance within Birmingham. Consequently, the application must be compliant with UK data protection laws and any pertinent local regulations specific to Birmingham. |

| **Describe the context of the processing:** what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)? |
| --- |
| The relationship is primarily indirect, as the data subjects (patients at incidents requiring medical assistance) do not directly interact with the application. Ambulance crew and other operational staff are direct users, with their data being processed to coordinate emergency medical responses efficiently.<br>Direct users (e.g., ambulance crew) will have some degree of control over their personal data, such as updating their availability or contact information. Patients, however, will have limited to no direct control over the data collected about them during medical emergencies. The application must ensure mechanisms for data subjects to exercise their rights under GDPR, such as accessing their data or requesting deletion, where applicable.<br>Individuals may reasonably expect their data to be used for the purpose of medical assistance and operational coordination during incidents. The explicit use of health and location data for dispatching resources and managing emergency responses aligns with these expectations. However, transparency about data processing activities is crucial to maintain trust.<br>Given the nature of the incidents covered, it is likely that children or other vulnerable individuals could be among those requiring medical assistance. This necessitates additional safeguards to protect their data, in line with GDPR's heightened requirements for vulnerable groups.<br>While not novel in its aim to improve emergency response efficiency, the application's approach to integrating live location tracking and real-time data processing could present novel aspects compared to existing technologies. Prior concerns in similar systems may include data breaches or inadequate protection of sensitive health data. Awareness and mitigation of such concerns are essential.<br>The technology for real-time data processing and location tracking is well-established, but continuous advancements necessitate keeping the application updated and secure. Public concerns often revolve around privacy and health data security, especially due to high-profile data breaches in similar contexts. Addressing these concerns proactively is vital.<br>The project is not yet signed up to any approved code of conduct or certification scheme under GDPR. However, exploring relevant schemes, once available, would strengthen the project's commitment to data protection and best practices. |

**Describe the purposes of the processing:** what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

AmbuDispatch is a web-based tool crafted specifically to enhance the quality of patient care and operational efficiency within Saint John Ambulance at incidents. By meticulously selecting resources based on their current priorities, locations, and availability, the application aims to dispatch medical services more swiftly, thereby ensuring quicker response times. It also enables seamless communication between field operatives and control centre staff, enhancing coordination for emergency responses. AmbuDispatch provides decision-makers with critical information needed for improved operational awareness and decision-making, offering a comprehensive view of incident operations. Moreover, by addressing existing system accessibility issues, the software focuses on user experience, reducing operational stress and the likelihood of errors. AmbuDispatch is expected to significantly reduce emergency response times for those in need, enhancing their wellbeing and potentially saving lives. It will also reduce the workload on ambulance crews and support staff, leading to more streamlined operations. For Saint John Ambulance as an organisation, AmbuDispatch promises enhanced efficiency in emergency response services, adherence to operational and legal requirements, and improved staff morale due to better working conditions. AmbuDispatch has a profound societal impact; it sets new standards for the integration of technology in emergency medical services and underscores a commitment to leveraging technological advancements for the betterment of community safety and public health.

## Step 3: Consultation process

**Consider how to consult with relevant stakeholders:** describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Consulting stakeholders is a crucial part of the DPIA process for AmbuDispatch, ensuring the application meets user needs while adhering to regulatory standards. Given the urgent nature of data collection in emergencies, direct consultation with patients isn't practical. However, operational staff and ambulance crews can offer invaluable feedback. By engaging these direct users through workshops, surveys, and testing sessions from the early stages of development and consistently thereafter, AmbuDispatch can effectively incorporate their insights on usability, accessibility, and privacy concerns.

Including a range of internal stakeholders within AmbuDispatch is also vital. This involves collaborating with the IT department to guarantee technical feasibility and integration, aligning with the operational leadership for strategic direction and feature prioritisation, working with the Data Protection Officer to ensure GDPR compliance, consulting the legal team on processing implications, and considering

the human resources department's insights on staff welfare. Regular interactions with these internal groups will foster a thorough understanding of the project's impacts and requirements.

Engaging with external experts and third-party processors is deemed crucial, especially for data security and protection measures. Their expertise will influence the application's design and any data processing adjustments. Information security specialists, in particular, play a key role in implementing sophisticated security measures to safeguard sensitive information.

Though direct patient interaction is minimal, AmbuDispatch is designed with a deep respect for patient privacy and dignity. This balanced approach of expert and stakeholder feedback aims to ensure AmbuDispatch is a robust, effective, and compliant tool, enhancing the operational capabilities of emergency response teams.

# Step 4: Assess necessity and proportionality

**Describe compliance and proportionality measures, in particular:** what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

AmbuDispatch processes personal data when necessary to perform tasks in the public interest, aligning with Saint John Ambulance's official duties. This involves overseeing medical services and ensuring the highest standards of care and security. The system is specifically designed for the rapid dispatch and management of emergency medical services, a critical aspect of real-time response, rendering manual or simpler methods inadequate for such pressing requirements. To prevent the system's misuse beyond its intended use, AmbuDispatch enforces strict user permissions and access controls, accompanied by regular audits and a thorough review process for any suggested modifications to the system's functionalities.

The integrity of the data is preserved through rigorous validation checks during data entry, complemented by user training to enhance accuracy. Built on the principle of data minimisation, AmbuDispatch ensures only the necessary information for emergency response activities is collected. Individuals are informed about the usage of their data through clear, accessible privacy notices, and AmbuDispatch supports their rights to access, correct, or delete their information by integrating functionalities that enable users to effectively manage such requests.

Processor agreements reflect GDPR standards, with due diligence and periodic audits conducted to ensure compliance with data protection laws and specific security standards. While primarily utilised within Birmingham, any international data transfers by AmbuDispatch will adhere to GDPR safeguards like adequacy decisions or Standard Contractual Clauses, ensuring data protection during such movements. These measures collectively guarantee that AmbuDispatch operates within legal parameters, achieves its objectives, and upholds stringent data protection and individual rights standards.

# Step 5: Identify and assess risks

| **Describe source of risk and nature of potential impact on individuals.** Include associated compliance and corporate risks as necessary. | **Likelihood of harm** | **Severity of harm** | **Overall risk** |
|---|---|---|---|
| **Risk 1** | | | |

| | | | |
|---|---|---|---|
| **Source of risk:**<br>Governance and access control to the data AmbuDispatch stores<br><br>**Potential impact on individuals:**<br>Personal Data is accessed by someone who is not permitted to view such data.<br><br>**Threats that could lead to illegitimate access, undesired modification and disappearance of data:**<br>Unauthorised access to the data can lead to illegal processing of data, modification and loss of data.<br><br>**Any compliance or corporate risks?**<br>Risk of breach or GDPR and corporate procedures on information security.<br><br>**Where mitigations are required what are these?**<br>To mitigate the risk, we have implemented role based access control to the relevant data only. We have also configured an audit function, which will record who has accessed which data. This will be stored in the log. User's information is also wiped on 1st July 2024 to prevent issues in the future. | Remote | Severe | Medium |
| **Risk 2** | | | |
| **Source of risk:**<br>The risk of service downtime or unavailability due to technical failures, system errors, or cyber-attacks.<br><br>**Potential impact on individuals:**<br>Delays in dispatching emergency services, leading to potential harm or life-threatening situations for individuals in need of urgent medical assistance.<br><br>**Any compliance or corporate risks?**<br>Failure to meet the service level agreements and response time commitments outlined in contracts or agreements with healthcare providers or emergency service partners. This leads to a breach of contractual obligations, financial penalties, and damage to professional relationships.<br>Operational inefficiency resulting from service interruptions can lead to reputational damage and | Remote | Severe | Medium |

| | | | |
|---|---|---|---|
| erode public trust in AmbuDispatch's reliability. This causes loss of credibility and potential business disruptions.<br><br>**Where mitigations are required what are these?**<br>Implementation of robust technical infrastructure with redundancy and failover mechanisms to ensure continuous service availability. Regular testing and updates to identify and address vulnerabilities promptly. | | | |
| **Risk 3** | | | |
| **Source of risk:**<br>The risk of dispatchers lacking adequate training in the use of the dispatch system or not being sufficiently familiar with the operational protocols.<br><br>**Potential impact on individuals:**<br>Miscommunication, delayed response times, or errors in dispatching emergency services due to dispatcher confusion or mistakes.<br><br>**Any compliance or corporate risks?**<br>Failure to adhere to established operational protocols and procedures governing the dispatch process. This could cause a violation of internal policies, potential legal consequences, and reputational damage due to errors in service delivery.<br>Decreased operational efficiency resulting from dispatcher errors can lead to public dissatisfaction and a loss of trust in AmbuDispatch's ability to handle emergency situations effectively. This will decrease public trust, create negative publicity, and potential challenges in securing partnerships with healthcare providers.<br><br>**Where mitigations are required what are these?**<br>Adequate documentation will be provided on how to use the system. The user interface is straight forward and relatively easy to learn. Customer satisfaction surveys will be used to ensure any issues are mitigated before they become too large. | Possible | Minimal | Low |
| **Risk 4** | | | |

| | | | |
|---|---|---|---|
| **Source of risk:**<br>The risk of the dispatch system not being scalable enough to handle a sudden surge in emergency calls or events, such as during natural disasters or mass casualty incidents.<br><br>**Potential impact on individuals:**<br>Delays in response times, overwhelmed dispatch system, and potential inability to efficiently handle a large volume of emergency requests.<br><br>**Any compliance or corporate risks?**<br>Failure to comply with SLAs and regulatory requirements related to response times and system reliability during peak periods. The potential impacts of compliance are a breach of contractual obligations, regulatory scrutiny, and potential legal consequences for failing to meet required standards.<br>An inability to handle high call volumes could result in negative publicity, damage to AmbuDispatch's reputation, and loss of public trust in the reliability of emergency services.<br><br>**Where mitigations are required what are these?**<br>Conduct regular scalability testing to ensure the dispatch system can handle increased loads. Implement redundancy plans and collaborate with technology partners to quickly scale resources during peak demand. | Remote | Severe | Medium |

# Step 6: Identify measures to reduce risk

| **Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5** | | | | |
|---|---|---|---|---|
| **Risk** | **Options to reduce or eliminate risk** | **Effect on risk** | **Residual risk** | **Measure approved** |
| Governance and access control to the data AmbuDispatch stores | Authenticate all routes. | Reduced | Low | Yes |

| | | | | |
|---|---|---|---|---|
| The risk of service downtime or unavailability due to technical failures, system errors, or cyber-attacks. | Have a backup service which can be temporarily used in case of technical failures. | Reduced | Low | Yes |
| The risk of the dispatch system not being scalable enough to handle a sudden surge in emergency calls or events, such as during natural disasters or mass casualty incidents. | Leverage cloud-based infrastructure to allow for on-demand scaling of resources during peak periods. Cloud services can automatically allocate additional computing power, storage, and bandwidth as needed, ensuring the system's scalability. | Reduced | Low | Yes |

# Step 7: Sign off and record outcomes

| **Item** | **Name/date** | **Notes** |
|---|---|---|
| Measures approved by: | Thomas Burke 05/03/2024 | Integrate actions back into project plan, with date and responsibility for completion |
| Residual risks approved by: | Thomas Burke 05/03/2024 | If accepting any residual high risk, consult the ICO before going ahead |
| DPO advice provided: | Thomas Burke 05/03/2024 | |
| Summary of DPO advice: Develop a backup service in case of cyber-attacks, technical failures or system errors. Use cloud-based infrastructure to allow for scaling in case of a sudden surge in emergency calls. Authenticate all routes to minimise the risk of a data breach. | | |
| DPO advice accepted or overruled by: | Ted Parting<br>05/03/2024 | Advice accepted |

| | | |
|---|---|---|
| Comments: DPO advice minimises the impact that risks will have on the service and is accepted | | |
| Consultation responses reviewed by: | Harvey Randall | |
| Comments: | | |
| This DPIA will kept under review by: | Thomas Burke<br>05/03/2024 | |