AUGMENTIA

Data Protection Impact Assessment

Data Protection Impact Assessment

This DPIA has been carried out at the start of this major project involving the use of personal data as it has the potential to result in significant change to existing processes. The final outcomes will be integrated back into the project plan.
It is the responsibility of the data controller to ensure a DPIA is carried out. A data processor can assist in the completion of a DPIA where it is responsible for the relevant processing operation, but the controller remains responsible for the DPIA. This DPIA has therefore been designed to assist data controllers with their requirements relating to the completion of a DPIA.

Organisation: Augmentia
Issue Date: Aug 11, 2025
Document Owner: Alex Radcliffe

Document Version Control

Version	Date	Description	Author	Approver
1.0.0	11/08/25	Initial release	Alex Radcliffe	Steve Marsh

Contents

Data Protection Impact Assessment

Pre DPIA-Checklist

Complete this section for proposed new projects that will involve processing personal data, to determine whether the project has data protection risks that need to be assessed with a DPIA.

Project Description	An automated back-office tool that helps GP practices to capture missed framework revenue with minimal admin effort.
Date	11/08/2025

	Question	Y/N
1	Are you based in the UK/EEA and processing personal data, or outside the UK/EEA and processing personal data of UK/EEA data subjects?	Y
2	Do you think the project is likely to result in a high risk to the rights and freedoms of the individual in relation to their privacy?	N
	Does the project involve…	
3	Evaluation or scoring	Y
4	Use of innovative technology	Y
5	Automated decision-making with significant effects	Y
6	Systematic monitoring	Y
7	Processing of sensitive data or data of a highly personal nature	Y
8	Processing on a large scale	Y
9	Processing of data concerning vulnerable data subjects	Y
10	Innovative technological or organisational solutions	Y
11	Processing that involves preventing data subjects from exercising a right or using a service or contract	N
12	Process biometric or genetic data in combination with any of the criteria in the European guidelines	N
13	Process personal data without providing a privacy notice directly to the individual	Y
14	Process personal data in a way that involves tracking individuals' online or offline location or behaviour	N
15	Use of systematic & extensive profiling or automated decision-making to make significant decisions about people	Y
16	Processing special-category data or criminal-offence data on a large scale	Y
17	Systematically monitoring a publicly accessible place on a large scale	N
18	Use of profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit	N
19	Carrying out profiling on a large scale	Y
20	Combining, comparing or matching data from multiple sources	Y
21	Processing children's personal data for profiling or automated decision-making or for marketing purposes, or offering online services directly to them	Y
22	Processing personal data that could result in a risk of physical harm in the event of a security breach	N

DPIA required if:	Two or more 'YES' answers to questions 3-14	Y
	One or more 'YES' answers to questions 15-22	
DPIA may be required if:	One or more 'YES answers to questions 1-14	Y
DPIA not required if:	All answers are 'NO'	N

Step 1: Identify the need for a DPIA

Project Name	Augmentia
Project Description	An automated back-office tool that helps GP practices to capture missed framework revenue with minimal admin effort.
Brief reason(s) why a DPIA should be carried out	The system systematically gathers & processes electronic health data on a large scale and evaluates the gathered data to create a dashboard for GP practices to check. Some of this processing is innovative. As such, a DPIA is required.
Name of Project Owner	Steve Marsh
Name of DPO	Alex Radcliffe

Step 2: Describe the processing

Describe the scope of the data being processed	
What is the nature of the data?	The data involved includes: Patient's email address, first name, last name, username or similar identifier, marital status, title, date of birth and gender, home address, email address, telephone numbers, NHS numbers, primary care health data, including those for the incidents falling under QOF, DES and LES frameworks.
What is the nature of the processing?	• Electronic patient records data will be accessed via NHS APIs such as IM1 and transferred in FHIR, or other appropriate formats to the Database of the application. • The dashboard of the application will be accessible by authorised GP practices and their clinical staff in order to display the required actions under QOF, DES, LES and any future or bespoke treatment frameworks. • The GP dashboard displays distilled metrics of this parsed information so GPs can make informed decisions about patient treatments and plan appropriate actions. • All data is encrypted in transit in between the application's infratructure, which includes IM1, Twilio, Cloudflare and other cloud or on-premises infrastructure which may be in use from time to time, and the GP Dashboard or end-user client. • All data is encrypted while at rest, including on the backend infrastructure and application databases. • Access to patient information is restricted to authorised GP practices and their designated clinicial staff and the Augmentia admins. • End-user access is secured by multi-factor user authentication provided by NHS supplied login systems (CIS2). Administrative accounts are secured with multi-factor authentcation alongside strong passwords stored as salted hashes in the applications database. No passwords are ever stored in plain text. • Augmentia uses regular testing in appropriate demo environments with synthetic information alongside penetration tests to verify that the system works securely and as intended.
Where will the data/processing be located (which country / countries)?	UK
Where are the data subjects based?	UK
How much data do you collect and use?	Full primary care patient records, which typically range from 1-100MB per patient.
How many individuals are affected?	On the order of tens of thousands of subjects.

Describe the context of the personal data	
What is the nature of your relationship with the individuals?	The individuals are patients of the GP practice(s); the GP practice(s) are Augmentia customers.
How much control will they have?	Individuals will not have control in relation to this data unless they opt-out from standard NHS data processing, as per the method is illustrated in Augmentia's privacy notice.
Would they expect you to use their data in this way?	The individuals can see how and with which purpose their data is processed by Augmentia in the relevant privacy notice.
Do they include children or other vulnerable groups?	Yes, as registered patients of GP practices, children and other vulnerable groups may be among the data subjects.
Are there prior concerns over this type of processing or security flaws?	We are not aware of any prior concerns over this type of processing or system security flaws.
Is it a different way of working in any way?	Yes, this is a new approach to unify all framework data into a single dashboard, allowing GP practices to easily trace their performance, complete treatment targets, and capture missed revenues from framework reimbursements.
What is the current state of technology in this area?	Immature
Are you signed up to any approved data protection code of conduct or certification scheme (once any have been approved)?	Covered by DTAC.

Describe the purposes of the processing	
What do you want to achieve?	This project aims to support GP practices in managing and maximizing their revenue opportunities under the NHS frameworks such as QOF, LES, and DES. Due to the complexity and administrative burden involved in coding, tracking, and submitting completed activities, GP practices often miss claiming revenues for tasks that were already performed. Our product resolves this by providing a cloud-based back-office admin tool that streamlines these processes.
What is the intended effect on individuals?	**Positive Effects:** *For GP Practice Staff (End Users):* **Reduced administrative burden**: Clinicians and administrative staff will spend less time on manual coding, tracking, and submissions, freeing them to focus more on patient care and core duties. **Improved financial oversight**: Staff responsible for NHS revenue submissions will have real-time visibility of missed or pending actions, improving efficiency and financial outcomes. **Enhanced usability and accuracy**: The system guides users through complex frameworks, reducing the risk of human error and simplifying compliance with NHS requirements. **Less stress and overwork**: By minimizing overtime related to tracking and submissions, the system can improve job satisfaction and reduce burnout. *For Patients (whose data is processed):* **Indirect improvements in care quality**: While the system does not interact directly with patients, increased administrative efficiency may lead to more clinician time available for patient-facing care. **Better data accuracy**: Integration with EPR systems reduces manual data entry, minimizing potential errors that could otherwise affect care planning or administrative outcomes. **Negative Effects:** *For GP Practice Staff:* **Learning curve**: Initial implementation may require training and adjustment time, especially for less tech-savvy staff. **Perceived surveillance**: The transparency and auditability of task tracking may cause anxiety among staff who feel they are being constantly monitored. *For Patients:* **Data privacy concerns**: Since patient data is used to generate dashboard actions and submissions, individuals may be concerned about how their data is being processed, stored, and accessed. *Mitigation:* The product includes safeguards against unauthorized access and ensures compliance with data protection standards to address this risk.
What are the benefits of the processing for you, and more broadly?	This procesing is essential for the functionality of the Augmentia product. When the product is deployed at scale the system will bring several broader benefits: **Improved efficiency in primary healthcare**: Reducing time spent on administrative tasks allows practices to operate more efficiently and potentially increase the availablity of patient appointments, improving access to care. **Increased NHS funding utilization**: By capturing all eligible claims under QOF, LES, and DES, practices can secure funding they are entitled to, ensuring better resource allocation, service delivery, and the long-term sustainability of Primary Care services. **Reduced public sector strain**: Automating back-office functions alleviates the staffing and workload pressures in GP practices, contributing to workforce sustainability in the NHS. **Data integrity and policy feedback**: More accurate and timely submissions help the NHS collect better data, which can inform health policy decisions and service planning. **Digital upskilling of healthcare workers**: Introducing intuitive digital tools contributes to a culture of innovation and capability-building within primary care teams.

Step 3: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular:	
Lawful basis	Augmentia is the processor of the data controlled by the NHS and GP Surgeries. The lawful basis for processing will be determined by the GP practices themselves, typically under Article 6(1)(e) (performance of a task in the public interest) and Article 9(2)(h) (health or social care purposes) of the UK GDPR.
Does the processing actually achieve your purpose?	Yes, the processing of personal data is necessary to achieve the project objectives. To identify missed revenue opportunities under NHS frameworks (QOF, DES, LES), the system must access and process patient-level data stored in GP practices' Electronic Patient Record (EPR) systems. This includes reviewing coded clinical activity, demographic data, and submission records to determine whether specific actions were completed and properly recorded for reimbursement. Without processing this data: The system would not be able to generate accurate, real-time dashboards for administrative staff. GP practices would continue to face manual burdens and risk missing claims despite having delivered the care. Importantly, the system does **not** use patient data for diagnosis, prediction, or direct clinical purposes. All processing is strictly limited to administrative and financial tracking, and is done under the authority and instructions of the GP practices, in compliance with data minimisation and purpose limitation principles.
Is there another way to achieve the same outcome?	Several alternative approaches were considered: 1. **Manual tracking and submission using Excel or internal systems** *Why not chosen*: This is the current approach used by many GP practices and has proven to be inefficient, error-prone, and time-consuming. It contributes to missed revenue opportunities due to inconsistent or delayed submissions. 2. **Standalone financial audit tools (without EPR integration)** *Why not chosen*: While this would reduce development complexity, it would not provide real-time insights or streamline submissions. It would still require manual data entry and cross-checking, negating much of the time-saving benefit and increasing risk of human error. 3. **Full outsourcing to external administrative services** *Why not chosen*: This may introduce greater data-sharing risks, in addition to being less scalable and flexible than an in-house digital tool and being financially less viable. 4. **Aggregated reporting based on anonymised patient data** *Why not chosen*: Anonymised data would not be sufficient to track individual submissions or match clinical actions to reimbursement claims, making the solution ineffective for the intended goal. The selected approach—integrated, dashboard-based software that uses patient data within the practice's secure environment—was chosen because it is the most efficient, scalable, and minimally disruptive method for improving operational and financial performance in GP practices.
How will you prevent function creep?	To prevent function creep, Augmentia has implemented a combination of technical, procedural, and contractual safeguards to ensure that personal data is only used for its explicitly intended purpose: enabling GP practices to identify and manage NHS framework-related administrative and financial tasks. **Controls and measures in place include:** **Purpose limitation by design** The software architecture is specifically designed to support only QOF, LES, and DES framework tracking and submissions. No features exist for diagnosis, treatment, or unrelated data analytics. Any future expansions or feature additions will go through a formal Data Protection Impact Assessment (DPIA) review. **Role-based access controls (RBAC)** Only authorized users (GP practice staff and specific Augmentia support personnel) have access to data relevant to their role. Admin privileges are restricted and logged to prevent unauthorized data use. **Data minimisation** The system only accesses and processes the minimum necessary patient data required to fulfill its administrative purpose. No irrelevant or excessive data fields are collected or stored. Processing is limited to the duration and scope defined by the GP practice. **Contractual and policy restrictions** Data Processing Agreements (DPAs) with GP practices clearly define the scope, purpose, and limits of data use, prohibiting repurposing without explicit controller consent. Staff are trained and bound by confidentiality and data handling protocols. **Audit trails and monitoring** All access and processing activities are logged to ensure transparency and accountability. Periodic audits and data protection reviews are conducted to detect any deviations from intended use. **No secondary use without consent** Patient data is not used for research, commercial analytics, or shared with third parties without explicit legal basis or patient consent. By embedding these safeguards, Augmentiaensures strict adherence to the principle of purpose limitation and protects individuals from the risks of privacy erosion through function creep.
Data minimisation	Augmentia applies the data minimisation principle as a core element of system design and operational procedures to ensure that only the minimum necessary data is processed to achieve the intended administrative functions. **Augmentia's approach includes the following safeguards:** **Requirement-based data mapping** Before development and during updates, Augmentia conducts a detailed mapping of the exact data fields required to support QOF, LES, and DES tracking and submissions. This ensures that the system minimises use of only the specific patient data relevant for providing the service. **No data collection outside of scope** The product does not collect or store data that is not directly related to Electronic Patient Records and delivering the NHS framework requirements. Sensitive or non-relevant categories of personal data (e.g., ethnicity, religion, or patient notes) are not accessed unless strictly required by the claiming framework. **Read-only and query-based integration** Where possible, the system uses read-only or query-level access to EPR systems, preventing unnecessary extraction or duplication of patient data. Temporary data views are used rather than storing full records, reducing exposure risk. **Governance and DPO oversight** Augmentia's Data Protection Officer (DPO) oversees data access protocols and reviews all new features or data-handling logic to ensure they align with the principle of data minimisation. DPIAs are conducted for significant changes to validate necessity and proportionality. **Continuous review and role-based limitation** The list of accessible data fields is routinely reviewed during product updates and client onboarding. Access to data within the tool is restricted based on user roles to prevent unnecessary exposure. By embedding these controls into the product lifecycle and governance structure, Augmentia ensure that personal data is collected and used **only to the extent necessary** to fulfil the project's administrative and financial efficiency objectives for GP practices.
Data quality	To maintain high standards of data quality throughout the system, Augmentia has implemented robust controls at every stage of data handling, particularly during transfer, integration, and usage. **1. Secure data transfer and integrity checks** Data is transferred between systems (e.g., from EPRs to the application) using secure, encrypted channels (e.g., HTTPS/TLS). Integrity checks such as checksums or hash verification are used to ensure that data is not altered, corrupted, or lost during transmission. The system performs validation checks to confirm that transferred data matches the source structure and content. **2. Synchronized and up-to-date data** The application does not store outdated snapshots but reads data directly or as near to real-time as possible from the GP practice's systems, ensuring current information is used in all dashboards and action prompts. Synchronization mechanisms are in place to refresh data regularly, and timestamping is used to track recency. **3. Accuracy and validation** Automated cross-checking logic ensures that submitted activities align with the rules of the relevant NHS frameworks (QOF, LES, DES). Where discrepancies are detected, the system flags them for review by authorized users before submission. **4. Role-based editing and logging** Only authorized staff within the GP practice can edit or update underlying records, helping to maintain data integrity. All changes are logged and auditable, ensuring traceability and accountability. **5. No unauthorised data merging** The product does not merge data from different patient records or systems unless explicitly required and authorized by the controller (the GP practice), reducing the risk of data mismatches or identity errors. Through these measures, Augmentiaensures that data used in the system is accurate, timely, consistent, and secure, supporting the reliability of NHS submissions and protecting patient information.
Data subject rights	A privacy notice will be provided to users (GP practice staff) at the start of their use of the system, outlining the nature of processing, purposes, and data protection measures. As Augmentia acts solely as a data processor for patient data, the legal obligation to inform patients lies with the data controller—i.e., the relevant NHS bodies or GP practices. However, to support transparency and best practice, Augmentia makes both its user-facing privacy notice and patient-related processing notice available on its website. This ensures that both data subject groups—practice staff and patients—have clear access to information about how their data is processed, even though the formal obligation to notify only applies to the data controllers.
How will you help to support their rights?	As a data processor, Augmentia is committed to supporting the rights of data subjects in alignment with the instructions of the data controllers—namely, the GP practices. The Augmentia platform is designed to facilitate these rights by ensuring data transparency, security, and access control. **Key measures include:** **Data access and portability support** Although data subject requests (e.g. access, rectification, erasure) are handled by the GP practices, the Augmentia system can be configured to help generate or export relevant data upon request from the controller, in a structured and readable format. **No restriction on controller rights management** The platform does not inhibit the GP practices from fulfilling data subject rights. All data is accessible to them for review, correction, and export, without proprietary locking. **Clear audit trails** Full activity logs are maintained, allowing the GP practice to respond to subject access requests with evidence of how and when data was accessed or used. **Data minimisation and purpose limitation** Since Augmentia only processes the data relevant to framework submissions, there is limited risk of using data in ways that would conflict with individuals' rights under GDPR. **Security to support the right to confidentiality and integrity** End-to-end encryption, access controls, and data integrity safeguards are in place to support the right to data security. **Processor obligations under contract** Augmentia's Data Processing Agreements (DPAs) include clauses requiring the company to fully support the controller in responding to data subject rights requests promptly and appropriately. **Conclusion:** While the GP practice remains the primary point of contact for data subjects, Augmentiaprovides the necessary tools, logs, and access structures to fully support them in fulfilling individuals' GDPR rights—such as access, rectification, objection, restriction, and portability—without obstruction or delay.
What measures do you take to ensure processors comply?	While Augmentia primarily acts as a **data processor**, in cases where **sub-processors** are engaged (e.g., cloud service providers or infrastructure partners), Augmentia implements the following strict measures to ensure full compliance with data protection laws and controller expectations: **Data Processing Agreements (DPAs)** Augmentia enters into legally binding DPAs with all sub-processors. These contracts clearly define the scope of processing, prohibit use beyond controller instructions, and impose obligations to comply with UK GDPR and relevant laws. **Technical and organizational safeguards** Augmentia requires all sub-processors to implement robust technical (e.g., encryption, access control) and organizational (e.g., staff training, policies) measures to ensure data confidentiality, integrity, and availability. Security certifications (e.g., ISO 27001, Cyber Essentials Plus) are preferred or required, where relevant. **Audit rights and monitoring** Sub-processor agreements include audit and inspection clauses, enabling Augmentia (or the controller) to review sub-processor compliance through audits or security documentation on request. Augmentia also conducts periodic reviews of security reports, performance, and risk exposure. **Data breach notification requirements** Sub-processors are contractually obligated to notify Augmentia immediately of any personal data breaches or security incidents, allowing the company to meet its obligations to the data controller in a timely manner. **Due diligence and risk assessment** Before engaging any sub-processor, Augmentia performs a formal due diligence process to assess their data protection practices, financial stability, and technical competence. The company maintains a register of sub-processors and provides suitable notice to controllers, allowing them to object if necessary. By taking these steps, Augmentia ensures that any third party processing data on its behalf does so with the same level of care, security, and legal compliance that the companys commits to as a primary processor.
Have you safeguarded any international transfers?	Augmentia has discussed the project with its legal and compliance teams. Where data is transferred outside the UK/EEA, it will ensure appropriate safeguards are used, including Standard Contractual Clauses or the UK's International Data Transfer Agreement, depending on the jurisdiction.

Step 4: Consultation process

Consider how to consult with relevant stakeholders:	
What was the feedback from data subjects?	The data subjects are patients of GP practices in England. Augmentia did not engage with them directly at this stage because the system is primarily designed for internal use by healthcare staff. While patient data is central to the system, it does not have patient-facing components incorporated to the product. However, we spoke extensively with those directly involved in patient care—GPs, practice leaders, practice managers, pharmacists, and admin staff—who shared valuable insights into both staff and patient challenges. Their feedback highlighted patient difficulties such as poor appointment coordination, lack of engagement, and missed care, which the system addresses through improved workflows, efficient reporting, and streamlined appointment scheduling. As a result of tracking the framework requirements for each patient, the patients will benefit through better access to care that is more efficiently delivered to them.
Who else has been involved internal or external and what was their feedback?	Augmentia has engaged with a wide range of stakeholders, including practice leaders, practice managers, GPs, pharmacists, and admin staff across GP practices, Primary Care Networks (PCNs), and Integrated Care Boards (ICBs). Their feedback consistently emphasised the need to reduce manual medical coding, improve appointment coordination, and track QOF, DES, and LES metrics in real time, while streamlining related workflows. Customers saw strong potential in the system to improve patient care, increase revenue, and automate tasks to help staff save time and work more efficiently. Overall, the system was viewed as practical, high-impact, and aligned with real needs in primary care.
What was the feedback from industry experts (e.g. security experts)?	The external and internal experts that were consulted during the development of the product played an active role in shaping the security and data protection approach. Their input directly informed decisions regarding system architecture, data flow design, cloud service selection, and encryption standards. Augmentia has implemented their recommendations to ensure the system remains secure, scalable, and appropriate for the intended operational scale. The adopted policies reflect current best practices in the sector, aligning with GDPR and NHS standards.
What is the feedback from the DPO?	Augmentia's DPO has played an active role in developing data security policies, from choosing the best tools to implementing them. In each stage of the product development, the DPO has reviewed and ensured that the appropriate steps have been taken.

Step 5: Identify and assess risks

Likelihood	Almost Certain	5	10	15	20	25
	Likely	4	8	12	16	20
	Possible	3	6	9	12	15
	Unlikely	2	4	6	8	10
	Rare	1	2	3	4	5
		1	2	3	4	5
		Negligible	Minor	Moderate	Severe	Catastrophic

Severity

High	Unacceptable, requires mitigation
Medium	Unacceptable, requires mitigation
Low	Acceptable, consider mitigation

Data Protection Principles

Category	Description (For information only; examples to consider when filling the next table)
Lawfulness, fairness and transparency	Augmentia will act as a *data processor*. The lawful basis for data processing is established by the GP practices (controllers). They typically rely on Article 6(1)(e) and Article 9(2)(h) of UK GDPR. **Data Processing Agreements (DPAs)**: We will have DPAs in place with all GP practice clients. These clearly define our role, obligations, and limits on data use. **Fairness & Transparency**: We only process data for clearly defined, contractually agreed purposes. We support controllers in meeting their transparency obligations, such as responding to subject access requests or exporting data. **Privacy Notices**: Augmentia does not process data without the knowledge of the controller. It is the GP practice's duty to provide patients with an appropriate privacy notice. We support them as needed (e.g., by documenting our role). **Sub-processors**: All sub-processors are listed in the DPA addendum. Controllers are notified prior to onboarding any new sub-processor. **International Transfers**: If data is stored or processed outside the UK/EEA, we use SCCs and/or UK IDTAs. Due diligence and International Data Transfer Assessments are conducted where applicable. **Cookies & Trackers**: In cases that we have cookies & trackers in the app or the commercial website, we have consent banner in place for users to opt. **Legitimate Interests**: Not applicable, as we are not the controller. Legitimate interest balancing tests would fall under the responsibility of the GP practice, if applicable.
Purpose limitation	Data is only used to support QOF, LES, and DES claims as outlined in the project scope. There is no repurposing for marketing, analytics, or other unintended functions.
Data minimisation	Only the minimum necessary data required for providing the service will be accessed. No unnecessary patient data fields will be stored or processed.
Accuracy	Data is accessed in real-time or near-real-time from the EPR, ensuring it reflects the most current state. Built-in validation and cross-checking routines help identify missing or inconsistent records before submission.
Storage limitation	Data is not stored longer than necessary. Most data is processed temporarily or cached in memory for current actions. Retention policies follow controller instructions and are included in contractual terms.
Accountability	Processing activities are documented. Staff receive data protection and security training. Security policies, audit logs, and access controls are enforced to ensure compliance and traceability. ROPA (Record of Processing Activities): As a processor, maintain a record of all categories of processing activities carried out on behalf of a controller. For the employee health data and the special category data we control for the employment, we have additional policy documents. Employee Training: All relevant employees are trained on secure data handling, processor responsibilities, and confidentiality obligations.
Confidentiality	Role-based access control (RBAC) limits access to only those who need it. Logs and alerts are in place to detect unauthorized access. A breach would expose sensitive patient data; therefore, strong encryption and access policies are in place to mitigate this.
Integrity	Controls are in place to prevent accidental or unauthorized alteration of data (e.g., read-only access to certain fields, audit logging). Data is cross-referenced with the EPR to ensure correctness during submission.
Availability	The system is hosted on secure, redundant infrastructure to minimize downtime. If data became unavailable, practices could miss NHS submission deadlines, resulting in financial loss and operational disruption. Disaster recovery plans are in place to reduce this risk.

Risk assessment

[Link to Risk Register]

Step 6: Sign off and record outcomes

Item	Name/position/date	Notes
DPIA signed off by:	[Name: Position: Date:]	Integrate actions (new risk controls) back into project plan, with date and responsibility for completion
Residual risks accepted by:	[Name: Position: Date:]	If accepting any residual high risk, consult the ICO before going ahead. If medium, please explain why they are being accepted.
Feedback from the DPO:	[Notes from DPO]	DPO should advise on compliance, risk mitigations, and whether processing can proceed
DPO advice accepted or overruled by:	[Name: Position: Date:]	If overruled, there must be an explanation for reasons.
Comments:		
Consultation responses reviewed by:	[Name: Position: Date:]	If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will be kept under review by:	[Name: Position:]	The DPO should also review ongoing compliance with DPIA