Data Protection Impact Assessment

Risk Manager

Date: 14/03/2026

Juniper

Contents

Data Protection Impact Assessment (DPIA)

How to complete a DPIA

A DPIA must be carried out if new technology is being deployed or there is a change to the nature, scope, context or purposes of existing processing activities which meets any of the criteria below. There are guidance notes in Appendix A to assist you in completing the form.

Screening

The DPIA comes in two parts: the first part is a short screening questionnaire, which requires you to answer a set of questions to establish whether certain data processing operations, activities or processes will impact upon the rights and freedoms of data subjects.

Full DPIA Assessment

Where you have answered yes to one or more of the screening questions in Part 1, you must complete Part 2 to document the assessment of the impact of the processing activities.

Part 1

DPIA Screening

Describe the project/processing/system etc. and, if it is new or a variation to existing, explain why it is being introduced. Include the objectives of the processing.

Juniper's Risk Manager is a software platform used by schools and multi-academy trusts to manage estate compliance, operational risk, and administrative processes. The system enables organisations to record, monitor, and manage information relating to assets, compliance checks, maintenance requests, incidents, suppliers, contracts, policies, and risk registers through a single platform. It includes features such as dashboards, templates, and automated alerts to support oversight and reporting. The objective of the processing is to support schools and trusts in maintaining safe facilities, managing operational risks, and meeting regulatory and compliance obligations.

DPIA Screening Questions

Complete this section to help determine whether the processing is likely to result in a risk to the rights and freedoms of data subjects. Use the guidance in Appendix A to assist you. Where the answer is yes/true, indicate this in the relevant checkbox.

You should **consider** carrying out a DPIA if you plan to carry out any of the following:

☐ A major project involving the use of personal data;
☒ Deploy new software/application/technology;
☒ Evaluation or scoring;
☐ Systematic monitoring;
☐ Processing sensitive data or data of a highly personal nature;
☐ Large scale processing activities;

You **must always** carry out a DPIA if you plan to:

☐ Process special-category data or criminal-offence data on a large scale;
☐ Process personal data that could result in a risk of physical harm in the event of a security breach;
☐ Process personal data concerning vulnerable data subjects;
☐ Process children's personal data for profiling or automated decision-making or for marketing purposes, or to offer online services directly to them;
☐ Process biometric or genetic data;
☐ Systematically monitor a publicly accessible place on a large scale;
☐ Process personal data without providing a privacy notice directly to those affected;
☐ Process personal data in a way that involves tracking individuals' online or offline location or behaviour;
☐ Use systematic and extensive profiling or automated decision-making or special category data to make significant decisions about people including decisions on someone's access to a service, opportunity or benefit;
☒ Combine, compare or match data from multiple sources;
☒ Use innovative technology or technology in innovate ways;
☐ Processing that involves preventing data subjects from exercising a right or using a service or contract.

If **any** of the boxes above are ticked, a DPIA **must** be carried out. Complete and sign below then complete Part 2 of this form.

If none of the boxes above are ticked a DPIA is not required. Complete and sign below then forward this form to the DPO@junipereducation.org

Part 2

About the Processing

What data is being processed?

Tick all that apply

☒ Name and titles/job titles

☒ Other identifiers e.g. ID, username, etc.

☐ Personal address/postcode

☒ Business address/postcode

☒ Personal contact details, phone, email, etc.

☒ Business contact details, phone, email, etc.

☐ Bank details/financial information

☐ Employment details including salaries and benefits

☐ Absence data

☒ Performance data

☐ Next of kin

☐ Special Category data (race, religion, trade unions, health, disability, political opinion, sexual orientation, biometrics etc.)

☐ Criminal offences/convictions

☐ Information about behaviour

☒ Audio or video recordings (e.g. CCTV images) or photographs

☐ Location or ip data

☒ Other (please state below):

Risk Manager's Accident & Incident module tracks Date of Birth and Sex of the person involved in the event (these fields are not mandatory)

Who is the data about?

Tick all that apply

☒ Employees, former employees, or prospective employees incl. volunteers etc.
☐ Customers, former customers, or prospective customers
☒ Suppliers, former suppliers or prospective suppliers
☒ Members of the public

Describe the people whose data is being processed below. Include a description of the nature of the organisation's relationship with data subjects and whether the processing might include children or other vulnerable groups.

The organisation processes personal data relating to individuals it interacts with in the delivery of its services. This includes agency staff, residents, volunteers, pupils, employees, contractors, and members of the public. The relationship varies depending on the role (e.g. service users, staff, or visitors). The processing may include data relating to children (pupils).

Would the people whose data is being processed expect their personal data to be used in the ways envisaged? Include a justification if it is within their reasonable expectations.

Yes

Purpose of the processing

What are the aims of the processing? What does the organisation want to achieve from it? If the data is pre-existing, how will the new use/processing differ from the current use/processing?

To ensure the customer is operating a safe environment to any person operating on the site, and to also ensure the customer site is prepared for H&S audits / inspections.

Responsibility/Beneficiaries

Who in our organisation is taking responsibility for the processing? Who stands to benefit from the processing and how? What are the intended effects on individuals? How will they benefit?

Product Owner, Product Manager and support teams, will process data for support and product development activities.

Nature and context of the processing

Describe the processing activities and their purpose. Provide sufficient context to enable the reader to understand how and why the processing occurs. Include information about how data will be collected, used and stored; the scale size and frequency of processing as well as who will use the information and for what purpose(s). If the processing is novel in any way, please describe how.

There is no novel processing. The data is stored within a secure database and will only be used to support customer queries and used to improve the software development roadmap. Singular tables from the database will be extracted at a low frequency, on average once per quarter for development purposed.

Data is collected within the system via imports from the customer in both mass formats and singular formats.

IT Systems

What IT systems including hardware and software will be used for the processing?

Include data flows where possible that explain and visualise the processing activities and flow of data.

Customers will upload data via Excel and Google Sheet imports via their desktop or portable appliances.

Disclosure and Sharing

Will the data be shared with any other people/organisations such as government agencies, data processors or sub-processors e.g. third party suppliers, application/website hosting companies, etc? ☐Yes ☒No

If yes, please list them below and include the purposes of the processing, their country and a link to their privacy notice.

Name	Purpose of processing	Country	Privacy Notice Link
Juniper Education – Risk Manager	Contract	UK	Privacy policy

Consultation Process

The purpose of a consultation process is to understand the concerns and expectations of the individuals, test appropriate solutions and improve transparency.

Will the organisation be seeking the views of staff/customers/residents/other stakeholders regarding this processing? If not, why is this not necessary? If yes, describe the consultation process.

Consultation with staff, customers, residents, or other stakeholders is not required because the processing undertaken through Risk Manager is limited to internal organisational use by authorised users under defined contractual terms, with no public-facing or externally impactful processing involved

Who else within the organisation will be consulted to ensure that all risks from the envisaged data processing are understood and properly mitigated?

This would typically include the Data Protection Officer, Group Information Security Officer and relevant business/data owners of the information being processed.

Assessing the processing's necessity and proportionality

Are there alternative solutions which meet the goals without creating the same data processing risks? For example, a high-risk data processing activity which carries minimal benefit for individuals or significantly affects their data protection rights may not be proportionate. Further, if there is a feasible alternative which is of lower risk (e.g. one that makes less use of personal data), such activity may also not be necessary.

☐Yes ☒No

If there are no alternative solutions, consider whether the data processing complies with the data protection principles.

Rights

Where Juniper is the Data Controller, they are responsible for all data subjects' rights request. Where Juniper is processing customer data e.g. to provide software or services, they are the Data Processor.

Who is responsible for responding to data subjects' rights requests?

The data controller (Juniper customer) is responsible.

Privacy Information

Does the Juniper Privacy notice provide sufficient information about how the data will be obtained and processed? If not, please contact DPO@junipereducation.org to have it added.
☒Yes ☐No

Lawful Basis

What is the lawful basis for processing the data? Tick all that apply

☐ Consent	☐ Vital interests	☐ Task by a public authority
☒ Performance of a contract	☐ Legal obligation	☐ Legitimate Interests

Is special category data processed? Special category data reveals racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic data; biometric data (where used for identification purposes); health; sex life; and sexual orientation.
☐Yes ☒No

If yes, what is the lawful basis for processing the special category data?

☐ Explicit consent	☐ Social security/protection law	☐ Legal defence or claim
☐ Employment law	☐ Vital interests	☐ Substantial public interest
☐ Public health interests	☐ Preventative/occupational medicine	☐ Archiving in public interest
☐ Data manifestly made public by data subject	☐ Scientific/historical research or statistical purposes	

Purpose Limitation and Minimisation

What measures have been taken to ensure that any personal data collected or created in this processing is not used for any purpose other than that documented in this DPIA?

Secure devices are the only methods to access data. Access to customer data via the database and via the application front end are protected by secure VPN access as well as additional database permission keys.

What measures have been taken to ensure that only adequate and relevant information is used in the processing and that it is limited to only that which is necessary to achieve the processing aims?

A robust permission set under 'Roles' in the system allows the customer to determine which areas users can collect data from via exports.

Accuracy

What measures have been taken to ensure that personal data is accurate? Is there a requirement to keep any personal data up-to-date? Could there be any negative consequences if the personal data is not kept up-to-date?

Onus on data controller (customer). No additional measures required and no negative consequences.

Storage Limitation (Retention)

What is the retention period for the various types of personal data? If you cannot specify a specific retention period, what are the criteria that determine if the information is no longer needed, e.g. fulfilment of contract? How will the information be treated, e.g. returned/destroyed when it reaches the end of its retention period?

90-day retention period which is outlined within our off-boarding policy. During the off boarding we will liaise with the customer to support with exporting all system data.

Upon termination of the contract, customer data may be deleted unless the customer submits a written request for its return or as specified in the contract.

Security

Describe the security measures that will be implemented to ensure the confidentiality, integrity, availability and restorability of the data, data systems and processes?

Risk Manager is owned and operated by Juniper Education, part of the wider Juniper Group. Juniper Group's systems benefit from the overarching information security governance practices, which holds a certified ISO/IEC 27001:2022 Information Security Management System (ISMS) and covers core applications/products, infrastructure, software development lifecycle, planned penetration testing, incident response, BCP/DR, cyber security operations, security awareness and training for all employees. The ISMS is formally audited yearly by external/approved organisation.

Juniper's security practices demonstrate implementation of a continuous security improvement framework covering:
Risk assessment & treatment
Asset management
Access control
Secure development lifecycle
Incident management
Business continuity
Supplier management
This compliments explicit technical & organisational security measures applied to Risk Manager including:

Ensuring confidentiality, integrity, availability and resilience
Timely restoration of personal data
Ongoing evaluation of security controls
Use of pseudonymisation and encryption where appropriate.

Risk Manager processes data on servers located in the United Kingdom and backup data is processed in Ireland.

Risk Manager is hosted on Microsoft Azure, which provides a highly secure and compliant cloud infrastructure. Azure maintains internationally recognised certifications, including ISO/IEC 27001 for its information security management system, ISO/IEC 27017 for cloud-specific security controls, ISO/IEC 27018 for protection of personally identifiable information in cloud environments, ISO 22301 for business continuity, ISO 9001 for quality management, ISO/IEC 20000 for IT service management, and PCI DSS for secure handling of payment-related data. These certifications and Azure's multi-layered security architecture strengthen the overall security, resilience, and compliance of the Risk Manager hosting environment.

Risk Manager follows a defined back-up policy that includes structured archiving and recovery processes, and uses reasonable endeavours to restore customer data from the most recent backup in the event of loss; upon termination of the contract, customer data may be deleted unless the customer submits a written request for its return or as specified in the contract.

Access to Risk Manager is restricted exclusively to authorised users, and the organisation retains the right to audit user accounts and access activity, while the customer is responsible for maintaining secure systems and connections to the platform.

Both parties are required to always maintain strict confidentiality, and all customer data processed within Risk Manager is explicitly recognised as confidential information
Customers must not transmit or introduce any malicious code, including viruses, into Risk Manager, and Risk Manager reserves the right to disable access to any harmful or otherwise prohibited content.

In the event of a data breach, affected customers will be notified without undue delay in line with Data protection legislation.

Customers are required to maintain secure networks and systems, prevent any unauthorised access to Risk Manager, and ensure that all data processed within the platform is handled lawfully and with integrity.

Juniper

WE LOOK AFTER YOU, SO THAT YOU CAN LOOK AFTER OUR CHILDREN

Junipereducation.org