ContractPodAi®

ContractPod Technologies Ltd.

GDPR Audit Report

July 2023

ShieldByte Infosec

Executive Summary

Scope	GDPR Audit
Audited By	Vaishali Mutalik CISA, CDPSE, CRISC, CPISI, CNSS, GDPR
Audit Team	Vaishali Mutalik Samiksha Jadhav Kajol Nhavkar
Auditee Representative	Michael Weaver Rokisha Lewis Shonda Bush
Period/ Dated	July 31, 2023
Audit Frequency	Annual Audit
Submitted To	▪ Viraj Chaudhary Chief Operating Officer ▪ Anurag Malik Chief Technical Officer ▪ Michael Weaver Director of Information Security

CONTENTS

Section – I
GDPR Auditor Report

Purpose

The General Data Protection Regulation (GDPR) came into force on May 25, 2018, replacing the Data Protection Act 1998 (DPA 1998).

The GDPR regulates the processing of personal data, which includes the collection, recording, organization, structuring, storage, alteration, retrieval, consultation, use, and disclosure by transmission, dissemination, combining with other data, restriction, erasure, or destruction.

The GDPR applies to computerized or manual records containing personal information about living and identifiable people and requires that appropriate technical and organizational measures be implemented to ensure compliance with the regulation. Data processors can process personal data unless the Data Controller (organization alone or jointly with others, determining the purposes and means of processing personal data) has identified an appropriate legal basis or bases which meets the requirements of the GDPR. The GDPR provides derogations to EU member states on some elements of how Data Protection law will work domestically. The UK has enacted the Data Protection Act 2018 for this purpose. The DPA 2018 also sets the law around types of personal data processing not covered in the GDPR (for example, the processing of personal data for law enforcement purposes).

The legislation introduces several significant changes to former data protection legislation, including, but not limited to, increased accountability and transparency requirements, strengthened rights for individuals concerning their data, and more significant penalties for breaching the needs of the Data Protection legislation, up to a maximum of €20 million or 4% of global turnover whichever is higher.

ContractPods' role is as the data processor and is primarily engaged with the data controller for the contract lifecycle management platform. ContractPod is not directly involved with EU data subjects and does not hold, obtain, or process any PII data except for EU employees.

This audit's objective was to ensure that ContractPod has adequate arrangements in place that are understood throughout the organization to protect ContractPods' information.

The factual accuracy of this report and action concerning the audit recommendations were discussed and agreed with Michael Weaver (Director of Information Security).

Audit Objectives and Scope

The overall objective of the audit was to evaluate and effectiveness of controls over the following areas:

- An assessment of plans in place to address GDPR that came into force in May 2018
- Assessment of action plan(s) in place to comply with the new regulation to ensure compliance with regulation

The audit also included a review of critical areas stipulated within Article 5 of GDPR, which requires personal data shall be:

- Processed lawfully, fairly, and in a transparent manner concerning individuals
- Collected and used for specified, explicit and legitimate purposes
- Adequate, relevant, and limited to what is necessary concerning the purposes of data processing
- Accurate and, where necessary, kept up to date (including taking every reasonable step to ensure inaccuracies are erased or rectified)
- Kept in a form that permits identification of data subjects for no longer than necessary. Data retentions include not storing information for longer than necessary; and
- Data processed, ensuring appropriate security over personal data.

The scope of the audit encompasses the evaluation of the adequacy and effectiveness of ContractPod GDPR Compliance.

Audit Scope	Description
Governance & Accountability	The extent to which information governance accountability, policies and procedures, performance measurement controls, and reporting mechanisms to monitor data protection compliance to both the GDPR and national data protection legislation are in place and in operation throughout the organization.
Training & Awareness	The provision and monitoring of staff data protection records management and information security training and the awareness of data protection regulation requirements relating to their roles and responsibilities
Data Sharing and Data Retention	The design and operation of controls to ensure the sharing of personal data complies with the principles of all data protection legislation.

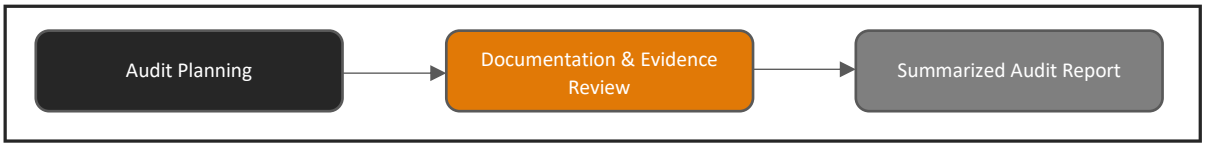
The scope covers the ContractPod UK office locations:

1. London, UK
2. Glasgow, UK

Audit Methodologies

The audit methodologies adopted to perform the GDPR audit:

- Discussions and interviews with the representatives from respective functional areas to understand the business processes of data acquisition, retention, and disposal.
- Review of operations activities relating to business processes and services offered.
- Review the effectiveness of related documents, policies, and records.
- Walkthrough of processes and systems within all business activities carried out at ContractPod.
- Analysis of the samples based on the risks identified and examining corroborating documents.



Management of Risk

The GDPR Audit process considers risks involved in the areas subject to review. Any risk implications identified through the GDPR Audit process are detailed in the attached appendix.

Information Security Responsibilities

Audit findings recommend that the Committee review, discuss and comment on the issues raised within this report.

Inherent Limitations

The opinion is based upon and limited to the work performed in respect of the subject under review. There are, on no account, direct financial and legal implications arising from the recommendations of this report.

Outcomes

There are no direct impacts, as a result of this report, concerning the Local Outcome Improvement Plan Economy, People or Place, or Enabling Technology, or on the Design Principles of the Target Operating Model.

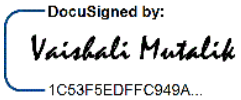
However, GDPR Audit plays a crucial role in providing assurance over, and helping to improve, the ContractPods' framework of governance, risk management, and control. These arrangements, put in place by ContractPod, help ensure that ContractPod achieves its strategic objectives in a well-managed and controlled environment.

Restricted Use

Shieldbyte Infosec respects the value and ownership of information they receive and does not disclose information without appropriate authority unless there is a legal or professional obligation.

This report is not intended to be used by anyone other than these specified parties.

Audited by:



Vaishali Mutalik
CISA, CDPSE, CRISC, CNSS, CPISI, GDPR

Section – II
Audit Summary and Findings

Audit Findings

Written Procedures and Training

Comprehensive written procedures and guidance, which are easily accessible by all staff members, can reduce the risk of errors and inconsistency. They are beneficial for the training of current and new employees and provide management with assurance that correct and consistent instructions are available to staff, imperative in the event of an experienced employee being absent or leaving. They have increased importance when new systems or procedures are introduced.

On ContractPods' intranet ("the Zone"), the Service provides policy, procedures, and guidance for managing information – primarily through the 'Managing Information Handbook.' The Service has updated the policy, procedures, and advice to reflect the requirements of GDPR.

The Service has been made available through a corporate training program regularly conducted. Corporate training sessions covered the following information security topics:

- Service-specific changes to data protection law
- Members training on changes to data protection law
- Data protection impact assessments
- Information asset owner training
- Managing information session
- Updating privacy notices

Information Governance mandatory training completion rates are being updated to management periodically.

Data Protection Officer

The ContractPod being a data processor, is not directly/indirectly involved with EU data subject for defining processing activities of personally identifiable data and does not obtain or process any personally identifiable information data except data of EU office employees.

Privacy Notices

Under GDPR Article 13, where ContractPod does not collect personal data relating to a data subject. ContractPod executes the data processor agreement with the data controller, clarifies the purposes of the processing, the legal basis for processing, and the data subjects' rights concerning their data held by the Data Controller. The data privacy and information security agreement review and inspection of the document carried out during the audit and assessment of relevant documents. The privacy notice adequately described the personal data collected; types of processing; the legal basis for processing; and the rights of the individual concerning their personal data held by ContractPod.

Individual's Rights

Under GDPR, an individual has eight defined rights:

- The right to be informed (privacy notices)
- The right of access (subject access)
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- The right about automated decision-making and profiling

ContractPods' information security and data privacy policies confirm that ContractPod has implemented policies and procedures for each of the above rights. The information security policy refers to a data subject right where relevant policies are made available.

GDPR Audit obtained a listing of all requests for erasure, access, rectification, and data portability. Under GDPR, ContractPod must respond to such reasonable requests within one month of receipt. ContractPod may charge a fee if the data subject request is deemed manifestly unfounded or excessive.

Data Processors

GDPR Article 28 (3) requires that if the data controller uses a third party to process personal data (data processor,) a contract should govern the processing. The agreements are reviewed and updated using a risk-based approach, appropriately updated under GDPR Article 28, and approved by both parties. A recommendation has been made here for tracking purposes.

Data Protection Impact Assessments

ContractPod has a legal requirement to carry out a data protection impact assessment (DPIA) for any processing that is likely to result in a high risk to the rights and freedoms of individuals. Within the ContractPods' Information Security Policy and Data Privacy Policy are guidelines to ensure DPIA's are periodically reviewed. Further, ContractPod maintains an up-to-date register of all DPIAs in progress and completed, sequentially numbered, to facilitate progress tracking.

Since the introduction of GDPR, ContractPod has carried out DPIA in April 2022. The Information Security Officer reviewed and approved the completed DPIAs as appropriate.

Data Breaches

The Information Security Management Team (ISM), responsible for supporting and driving the broader information governance agenda, reviews ContractPods' data protection compliance quarterly. A report is reviewed quarterly by the ISM, which includes response times to data subject access and the number of data protection breaches and complaints. The data breaches are reported annually to the Audit, Risk, and Scrutiny Committee.

Information Asset Register

Article 30 of GDPR requires that each controller maintain a record of processing activities under its responsibility along with the data processed by the data processor. That record shall contain all of the following:

- The name and contact details of the controller
- The purposes of the processing
- A description of the categories of data subjects
- The categories of personal data
- The categories of recipients to whom the personal data have been or will be disclosed (including internationally)
- Details of transfers to a third country
- Time limits for erasure (where possible)
- Description of the technical and organizational security measures where possible

ContractPod maintains an Information Asset Register, which is found to be up to date. The processing activities recorded concerning personal data held were found to comply with the requirements of GDPR.

Data Retention

Article 5(1)(e) of GDPR requires that data not be held when needed. The Data discovery process and DPIA assessment have observed that and data captured for the contract lifecycle management. ContractPod is not capturing, obtaining, or managing any data pertaining to EU residents' "Data Subject" except employees of ContractPod.

Business Contracts

Given the sensitive high-risk nature of employee data, it is crucial to store these securely, and only authorized personnel can access them. GDPR Audit team reviewed and audited employees' data of data subject. Inspections are undertaken to ascertain how personal data is collected and stored and ensure that personal data is stored securely and only accessible by authorized individuals. Exceptions have not been observed concerning data security.

ContractPod does not collect personal data, including particular category personal data, of Data Subject. The business agreement clearly defines the sharing of personal data with partners of ContractPod, based on data-sharing agreements and a need-to-know basis.

Data Disposal

Electronic media waste, Media disposal policy, defined, established, and implemented for compliance. Data storage arrangements were found to be adequate.

Freedom of Information

Under the GDPR Regulation, the data subject is entitled to request information held by ContractPod. However, when providing this information, ContractPod must ensure that data protection legislation has complied. GDPR Audit examined the procedures in place for responding to FOI requests to ensure this complied with data protection requirements. ContractPods' website was reviewed to ensure these complied with data protection legislation. No significant exceptions were observed during the audit, and the strategies were proper.

Data Sharing

ContractPod holds data-sharing agreements with organizations for business process agreements. Therefore, the conclusion or updating of such contracts will often depend upon input from several different parties. Each agreement is tracked on an Information Sharing Agreement Register identifying all parties involved. During the review of privacy notices, it was confirmed that these sharing agreements are being appropriately disclosed where required. Further, the Service is reviewing these Information Sharing Agreements to assess whether or not they comply with GDPR.

Audit Recommendations

1. Third-Party Vendor (Processor \ Sub Processor) Audit	
Control Weakness	**Risk**
The IT vendor assessment and audit for GDPR compliance were not executed.	Vendors (sub-processors) engaged for services.
Findings	**Priority Level**
Contractually binding agreements exist between Contractpod and their third-party suppliers that outline the. The contract agreements with vendors are reviewed annually.	**MEDIUM**
Recommendations	**Timescale**
It recommended that ContractPod conduct third-party vendor assessment and audit yearly for the existing vendors before appointing new vendors. The audit should cover ▪ Data retention and data disposal of backup copies of records in accordance with business, contractual and regulatory requirements. ▪ A representative from ContractPod legal function should validate the minimum retention period identified by the relevant business functional heads; ▪ The local data protection regulation and data disposal evidence ▪ Data Protection Impact Assessment of Vendor. ▪ Data breach reporting readiness and timelines.	31.10.2023

Audit Summary Findings

We confirm, to the best of our knowledge and belief, that ContractPod has taken the necessary actions to ensure that they are compliant with GDPR and have implemented monitoring arrangements to ensure that they remain compliant. The controls implemented provide satisfactory assurance at an acceptable level.

Limited	**Satisfactory**	Substantial
There is a risk of objectives not being met due to serious control failings.	A framework of controls is in place, but the management of control requires strengthening.	There is a robust framework of controls that are applied continuously.

The factual accuracy of this report and recommendations have been agreed upon with ContractPod Management Team. The audit report is valid till July 31, 2024.

DocuSigned by:
Vaishali Mutalik
1C53F5EDFFC949A...

Vaishali Mutalik
Principal Auditor
CISA, CDPSE, CRISC, CPISI, GDPR

Section – III

Data Protection Impact Assessment – DPIA

Data Protection Impact Assessment – DPIA SCOPE

Shieldbyte Infosec Pvt. Ltd. was engaged to review the Data Protection Impact Assessment (DPIA) carried out under the GDPR regulations. The Shieldbyte Infosec completed DPIA, and a review was performed on the documents and evidence submitted by ContractPod for review and assessment.

The purpose of the review was to determine that ContractPod has assessed its privacy risks and has adequate controls in place to mitigate them. The review of the DPIA is not a comprehensive review of GDPR compliance but an assessment of the adequacy of the inputs forming part of the DPIA.

The regulatory scope of this report is limited to the General Data Protection Regulation (GDPR).

Review Methodology

The following are the procedures and review methodologies adopted to perform the assignment.

- Discussions and interviews with the management to understand the processes
- Review of operations activities relating to business processes and services offered
- Inspection of related documents, policies and a review of the level and depth of content
- Walkthrough of processes and systems within all business activities carried out at ContractPod

Scope Limitation

Shieldbyte Infosec's DPIA review engagement was limited to evaluating the adequacy and completeness of the DPIA.

Shieldbyte Infosec is not liable for any incomplete or inaccurate information provided to us or any financial or non-financial loss due to our engagement and this report.

DPIA Assessment

		Yes	No	Unsure	Comments
i	Is the information about individuals likely to raise privacy concerns or expectations, e.g., health records, criminal records, or other information people would consider particularly private?	☒	☑	☐	Not Applicable as Consent from Data Subject is obtained by Data Controller and ContractPod being data processor only
ii	Will the initiative involve the collection of new information about individuals?	☒	☑	☐	ContractPod is not collecting any new information from data subjects.
iii	Are you using information about individuals for a purpose it is not currently used for, or in a way, it is not currently used?	☒	☑	☐	ContractPod, being a Data sub-processor, acts according to Data Controller's instructions.
iv	Will the initiative require you to contact individuals in ways they may find intrusive?	☒	☑	☐	Not Applicable as Consent from Data Subject is obtained by Data Controller and ContractPod being data processor only
v	Will information about individuals be disclosed to organizations or people without routine access to the information?	☒	☑	☐	No such engagement with Third-party and/or any individuals
vi	Does the initiative involve you using new technology which might be perceived as being privacy-intrusive e.g., biometrics or facial recognition?	☑	☒	☐	Initiatives do not involve the usage of any new technology.
vii	Will the initiative result in you making decisions or taking action against individuals in ways that can significantly impact them?	☒	☑	☐	Not Applicable as Consent from Data Subject is obtained by Data Controller and ContractPod being data processor only

Is DPIA Required?	Yes	No
	☑	☒

Data Protection Impact Assessment

Systematic Description of the Envisaged Processing Operations and Purpose

Project/Change Outline - Description	
What is it that is being planned? If you have already produced this as part of the project's Project Initiation Document or Business Case etc., you may refer to this. However, a brief description of the project/process being assessed is still required.	DPIA assessment, along with the Risk Assessment process carried out, has been observed that data captured during the business process is primarily of business transactions and required contract lifecycle management, ContractPod clients.
Purpose / Objectives	
Why is it being undertaken? This could be the objective of the process or the purpose of the system being implemented as part of the project.	The regular monitoring and maintenance task for the devices and to maintain maximum availability & uptime. The servers are located based on the geographical locations of the client. The devices are located at ContractPod global offices & Cloud platforms.
What is the purpose of collecting the information within the system? For example, patient treatment, administration, research, audit, reporting, staff administration, etc.	ContractPod engagement with the data controller is for the transformation of planning and operations. Considering the defined processing activities, the data processor does not have access to a database holding data of the data subject, and hence right to object will not be the responsibility of ContractPod.
Legal basis for the processing of personal data	1. The data controller obtains consent 2. ContractPod is legally bound with the customer not to misuse or share the data with any third party or external sources. 3. The legitimate interest is for the smooth functioning of the data integrity.
What are the interests pursued by us, like the Controllers or processors?	The interest pursued by ContractPod as a data processor is to protect the data shared by the controller to be maintained confidential and secured.
Use and Interface Specifics	Authorized users can be assigned roles that allow them to manage the data in a controlled environment effectively

Where is the data coming from? Describe the data flow of processing operations.	Our clients (Data controllers) provide the data for data migration and contract lifecycle management platform services and support.
What are the potential privacy impacts of this proposal - how will this change effect the data subject? Provide a summary of what you feel these could be, and it could be that specific information is being held that hasn't previously or that the level of information about an individual is increasing.	There are no specific fields or information which is captured. The Data Minimisation principle is implemented while capturing the information for defined business processes.
Provide details of any previous Privacy Impact Assessment - or other forms of personal data compliance assessment done on this initiative. A PIA may have been undertaken during the project implementation if this is a change to an existing system.	No previous PIA has been carried out earlier.
Stakeholders - who is involved in this project/change? Please list stakeholders, including internal, external, organizations (public/private/third), and groups that may be affected by this system/change.	ContractPod undertakes the project, and the management and staff members of ContractPod will be involved while dealing with the GDPR Compliance project. **Stakeholders:** ▪ Anurag Malik ▪ Viraj Chaudhary ▪ Michael Weaver

Assessment of Necessity and Proportionality

Describe the specified, explicit and legitimate purpose(s)	The lawful basis for Data usage is given below. Performance of Contract with Data Controller 1) Data Migration 2) Contract Lifecycle Management Platform 3) Application Support
Describe the lawfulness of processing for the category of data. Attach a separate document if necessary.	The data category is for data migration and contract life cycle management platform support as per projects/business contracts signed and terms agreed upon by the data controller. The only lawful basis is the performance of the contract.
Describe adequate, relevant and limited to what is necessary data	No other PII information is collected
Describe data retention policies for the data being processed. i.e., Limited storage duration	During the Data discovery process & DPIA assessment, along with the Risk Assessment process, it has been reviewed that the data captured do not contain any critical information pertaining to Data Subject. GDPR audit observations are that the data is captured in the data controller's system. ContractPod is not capturing or obtaining any data pertaining to EU residents' "Data Subject" except EU office employees. ContractPod has defined, established, Implemented & monitored Information Security policies & procedures for Information Security & Data Privacy.

Assessment of measures contributing to the rights of the data subjects

What are the information and privacy notices provided to the data subject? How are they offered?	As ContractPod is Data Processor, the provision of Information & Privacy notices is not under purview.
Does the processing also include the rights of portability of data	No, all the data managed is not portable and has to be accessed by Data Controller only.
How is the right to rectify or erase? Object, restriction of processing covered/addressed	As ContractPod is the data processor, it is covered by Data Controller with the customer.
Who are the recipients of data, both internally and externally	Internally – Only ContractPod dedicated staff on the project. Externally – None.
Identify all processors for the personal data being processed	There is no personal data that is processed except ContractPod employees of the EU region.
Identify all cross-border transfers across the lifecycle of the personal data. What are the safeguards surrounding it? International transfer(s)	Cross-border transfer does not apply in terms of data storage or transfer.

Privacy Compliance Assessment

Compliance Assessment	Response	Risks (Y/N)
Legal compliance – is it fair and lawful?		
What is the legal basis for processing the information? This should include which conditions for processing under the Data Protection Act 1998 apply and the common law duty of confidentiality.	1. ContractPod is an application provider for contract lifecycle management. Business Agreements are executed between Data Controller and ContractPod, the data processor. ContractPod is not directly/indirectly involved with EU data subjects & does not hold or obtained, or process any PII data except for ContractPod EU employees. 2. ContractPod is legally bound with the customer not to misuse or share the data with any third party or external sources. 3. The legitimate interest in the functioning of data privacy	N
Is processing an individual's information likely to interfere with the 'right to privacy' under Article 8 of the Human Rights Act?	No, it is not likely to interfere with the right to privacy	N
Have you identified the initiative's social needs and aims, and are the planned actions a proportionate response to the social need?		
Individuals affected by the initiative must be informed about what is happening with their information. Is this covered by fair processing information already provided to individuals, or is a new or revised communication needed?	Not Applicable as data of Data Subject is obtained by Data Controller and ContractPod being data processor only	N

If you rely on consent to process personal data, how will consent be obtained and recorded, what information will support the consent process, and what will you do if permission is withheld or given but later withdrawn?	Not Applicable, as Consent from Data Subject is obtained by Data Controller, and ContractPod is the data processor only.	N
Purpose		
Does the project involve the use of existing personal data for new purposes?	No, the personal data is not used for any new purpose except a data migration project guided by a duly executed business agreement with the data controller.	N
Are potential new purposes likely to be identified as the project scope expands?	No	N
Adequacy		
Is the information you are using likely to be of good enough quality for the purposes it is used for?	Yes	N
Accurate and up to date		
Are you able to amend information when necessary to ensure it is up to date?	Not Applicable	N
How do you ensure that personal data from individuals or other organizations is accurate?	ContractPod does not capture any personal data	N
Data Retention		
What are the retention periods for personal information, and how will this be implemented?	ContractPod, being Data Processor, does not capture any personal information. The data captured for EU employees are retained with the data retention principle, and consent for the same is duly obtained from Data Subject (EU Employees)	N
Are there any exceptional circumstances for retaining specific data longer than normal?	Not Applicable, ContractPod being the data processor, data retention is in accordance with the business agreement with the data controller, and there are no exceptional circumstances for retaining certain data for longer than the normal period.	N

How will information be fully anonymized or destroyed after it is no longer necessary?	Data destruction occurs across the systems after the information is no longer necessary. The Data destruction policy is duly implemented across ContractPod offices.	N
Rights of the Individual		
How will you action requests from individuals (or someone acting on their behalf) for access to their personal information once held?	Not Applicable, ContractPod being data sub-processor only.	N
Appropriate technical and organizational measures		
What procedures are in place to ensure that all staff with access to the information have adequate information governance training?	Information Security policy with Relevant Access Controls and Role, Responsibilities defined, established, and implemented.	N
What security measures are in place if you are using an electronic system to process the information?	Trace logs are being monitored & reviewed by the management	N
How will the information be provided, collated, and used?	The information is collated and used for information security and data privacy.	N
What security measures will be used to transfer the identifiable information?	ContractPod, a data sub-processor, has implemented a secured data transfer protocol to transfer identifiable information.	N
Internal and External Data Transfers, including outside EEA		
Will an individual's personal information be disclosed internally/externally in an identifiable form, and if so, to whom, how, and why?	Not Applicable, ContractPod, being data sub-processor only, does not obtain, process, and retain any personal information and is not disclosed internally and externally.	N
Will personal data be transferred to a country outside the European Economic Area? If yes, what arrangements will be in place to safeguard personal data?	Not Applicable, ContractPod does not capture and transfer personal data outside EEA.	N
Consultation		
Whom should you consult to identify the privacy risks, and how will you do this? Identify both internal and external stakeholders.	Director Information Security	N

What privacy risks have been raised? E.g., the Legal basis for collecting and using the information, the security of the information in transit, etc.	There are no risks that have been identified	N

Stakeholders' View of DPIA

Since this is not a complex process, stakeholder views were not taken to complete this DPIA.

Recommendations

Ref	Recommendation	Agreed Y/N
1	Data Processor and Sub Processor compliance assessment and audit	Yes

Conclusion on DPIA

Based on our review of the DPIA, we believe that the DPIA is comprehensive and covers all the critical factors that go into privacy assessments. The processing results in risks that are at an acceptable level.