BCNET

Shared Services for Higher Education & Research

Privacy Impact Assessment: Deem – Etta Travel Management Program

Table of Contents

PART 1: GENERAL INFORMATION

PIA file number:

Initiative title:	Deem – Etta Travel Management Platform
Organization:	BCNET
Branch or unit:	Procurement Services
Your name and title:	Jo-Ann Bellamy, Privacy Consultant Hooper Access and Privacy Consulting Ltd.
Your work phone:	250-208-3431
Your email:	jbellamy@hooperconsulting.ca

Initiative Lead name and title:	Dennis Silva Chief Procurement Officer
Initiative Lead phone:	604-412-7728
Initiative Lead email:	Dennis.silva@bc.net
Privacy Officer:	
Privacy Officer phone:	
Privacy Officer email:	

General information about the PIA:

Is this initiative a data-linking program under FOIPPA? If this PIA addresses a data-linking program, you must submit this PIA to the Office of the Information and Privacy Commissioner.
No.
Is this initiative a common or integrated program or activity? Under section FOIPPA 69 (5.4), you must submit this PIA to the Office of the Information and Privacy Commissioner.
No.
Related PIAs, if any:
N/A

1. What is the initiative?

BCNET is a federally incorporated not-for profit services and information technology organization that represents the interests of its member institutions comprised of 25 publicly funded universities, colleges, institutes, and research organizations across British Columbia. It represents all public, post-secondary education institutions in the province and provides shared services to its members in the areas of networks, procurements, licensing, and IT services.

BCNET is assessing Deem's Etta travel management platform on behalf of its member institutions. Etta is a mobile, cloud-based travel solution that allows employees to quickly shop for, book, and manage their travel. Etta's features include:

- Users can book or modify anything themselves from any device.
- Google's ITA search engine gives employees more airfare options, dynamic sorting, and quicker response times than GDS-only solutions.
- Health and safety information is built into the booking flow to help guide users to safer travel choices.
- Users can view flight seat maps and pin seats while cross shopping.
- No more screenshots: just hit share and keep shopping.
- Apply comprehensive travel policies and drive compliance without sacrificing user satisfaction.
- Compare fare tiers on one page—no clicking required.
- Connects seamlessly to most external expense platforms including Certify, Chrome River, Coupa, Infor, Workday, and more.
- Users are in 60+ countries, and the solution supports 14 languages.
- Apply customer and TMC negotiated rates for additional savings on every trip booked.

Personal information is collected from users when they set up their user profile in Etta. The personal data is stored and accessed outside of Canada in Sterling, Virginia and Santa Clara, California, USA. Users are prompted to consent to the storage of their personal information outside Canada before setting up their profile and entering personal information.

Deem uses the personal information to provide their services, communicate with users, and provide customer support. Deem may share data with their authorized third-party service providers for the purpose of providing and supporting Deem's services.

Deem has appropriate physical, technical, and administrative safeguards in place to protect users' personal information.

2. What is the scope of the PIA?

This PIA addresses the collection, use, disclosure, storage, access, and security of personal information in Deem's Etta travel management platform.

Member institutions may decide to complete a separate PIA on their use of the platform.

3. What are the data or information elements involved in your initiative?

Deem collects and processes personal information with the user's consent as required to meet their legitimate obligations such as providing services to customers, meeting contractual and legal requirements, ensuring compliance, and protecting the security of systems and customers.

The personal information collected includes:

- Contact information including name, address, phone, and email address
- Billing information which includes credit card details, customer employee ID, or other details required for purchase. (This is customer defined.)
- Travel preferences including preferred meals and seats and emergency contacts, known traveler number, special requests (meals, seating, hotel), default flight search requirements (fare types, search experience)
- Trip itinerary which includes confirmation number, travel destinations, and other preferences for booking transportation and accommodations (e.g., air special requests - visually/hearing impaired, wheelchair assistance, hotel special requests - away from elevator, higher floor, disabled access, care special request - mobile phone, cruise control, luggage rack, ski rack, navigation system
- Date of birth
- Expense reporting such as receipt images and information required for approval purposes. For expense partners – traveler name, travel booking details, and cost breakdown.
- Travel documents including visa details and passport number, redress number, known traveler number, gender, date of birth, and issue and expiration dates. Visa and

passport data is not automatically passed to the reservation and must be configured by the TMC with PNR edits).

- Loyalty information which includes frequent flyer numbers
- Information from our customer's financial or human resources systems. This varies by customer. Most companies pass, at minimum, groupware ID, username, name, phone number, and email. Any additional data, such as hierarchical information, is based on customer requirements.
- Web site activity, including but not limited to page views, whitepaper downloads and video views. Whitepaper downloads and video views refers to Deem.com and not company booking tool access. Traveler language preferences are collected.

In addition, when an individual visits Deem's websites or uses the mobile applications, they may collect certain information by automated means, such as cookies and web beacons. Deem may also use third-party website analytics tools that collect information about visitor traffic on their sites. The information they may collect by automated means includes:

- Information about the devices that website visitors use to access the Internet (such as the IP address and the type of the device, its operating system type and web browser)
- Search terms that visitors use to reach Deem websites
- Location information, such as the real-time geographic location of the device on which the visitor installs the mobile applications based on the visitor's consent

3.1 Did you list personal information in question 3?

Personal information is any recorded information about an identifiable individual, other than business contact information. Personal information includes information that can be used to identify an individual through association or reference.

Yes.

- If yes, go to Part 2
- If no, answer question 4 and submit questions 1 to 4 to your Privacy Officer. You do not need to complete the rest of the PIA template.

4. How will you reduce the risk of unintentionally collecting personal information?

N/A

PART 2: COLLECTION, USE AND DISCLOSURE

This section will help you identify the legal authority for collecting, using and disclosing personal information, and confirm that all personal information elements are necessary for the purpose of the initiative.

5. Collection, use and disclosure

Use column 2 to identify whether the action in column 1 is a collection, use or disclosure of personal information. Use columns 3 and 4 to identify the legal authority you have for the collection, use or disclosure.

Use this column to describe the way personal information moves through your initiative step by step as if you were explaining it to someone who does not know about your initiative.	**Collection, use or disclosure**	**FOIPPA authority**	**Other legal authority**
Step 1: User creates a profile in Etta which includes personal information	Collection	26(c)	
Step 2: Individuals search for travel options and make their preferred travel selections.	Collection	26(c)	

Step 3: User enters their payment card details which is encrypted and sent directly to the travel partner providing the services selected. Deem provides the user the ability to store their payment card details in which case it is written to a database and encrypted where it can be retrieved for future use.	Collection
	Use
		26(c)
		32(a)	

Use this column to describe the way personal information moves through your initiative step by step as if you were explaining it to someone who does not know about your initiative.	**Collection, use or disclosure**	**FOIPPA authority**	**Other legal authority**
Step 4: Deem uses the personal information to provide their services, communicate with users, and provide customer support.	Use	32(a)	
Step 5: Deem's third party service providers may use the data for the purpose of providing and supporting Deem's services.	Use	32(a)	

6. Collection Notice

If you are collecting personal information directly from an individual the information is about, FOIPPA requires that you provide a collection notice (except in limited circumstances).

BCNET member organizations are responsible for ensuring the appropriate notification is in place prior to the collection of personal information. Deem Etta users must indicate they accept the privacy policy before providing their personal information and registering to use the application. The content for the privacy policy reference is fully configurable so member institutions must include their collection notice in the content. Users will then provide their explicit consent before using the application.

PART 3: STORING PERSONAL INFORMATION

If you're storing personal information outside of Canada, identify the sensitivity of the personal information and where and how it will be stored.

7. Is any personal information stored outside of Canada?

Yes.

8. Does your initiative involve sensitive personal information?

Yes.

- If yes, go to question 9
- If no, go to question 10

9. Is the sensitive personal information being disclosed outside of Canada under FOIPPA section 33(2)(f)?

No.

- If yes, go to question 10
- If no, go to Part 4

10. Where are you storing the personal information involved in your initiative?

After you answer this question go to Part 5.

Personal information is stored in data centres in Sterling, Virginia and Santa Clara, California in the USA.

PART 4: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA

Complete this section if you are disclosing sensitive personal information to be stored outside of Canada. You may need help from your organization's Privacy Officer.

11. Is the sensitive personal information stored by a service provider?

Yes.

- If yes, fill in the table below (add more rows if necessary) and go to question 13
- If no, go to question 12

Name of service provider	Name of cloud infrastructure and/or platform provider(s) (if applicable)	Where is the sensitive personal information stored (including backups)?
Deem	Cyxtera	Sterling, Virginia, USA Santa Clara, California, USA

12. Provide details on the disclosure, including to whom it is disclosed and where the sensitive personal information is stored.

Personal information is disclosed to Deem who stores the personal information in secure data centres in Sterling, Virginia and Santa Clara, California, USA.

13. Does the contract you rely on include privacy-related terms?

Yes.

- If yes, describe the contractual measures related to your initiative.

BCNET does not hold an agreement directly with DEEM. Direct Travel (formerly Uniglobe) offers Deem as an extension of its services. This agreement has been reviewed and contains appropriate privacy related terms. BCNET Member Institutions must ensure that they review the privacy protection measures within that agreement as they may change from time to time.

15. What controls are in place to prevent unauthorized access to sensitive personal information?

BCNET

BCNET member institutions are responsible for the management and administration of user access within their institutions.

Deem

Access to production systems is limited to only those who have a need to know. This includes:

- Select individuals from systems administration, database administration, and network administration
- Select individuals from engineering have read access to system files and logs (but no user data) for supporting site production and troubleshooting
- Members of customer support are able impersonate users; in this role customer support staff have access to a limited subset of user information

Server administrators do not have access to sensitive data, and database administrators do not have administration rights on the database servers.

16. Provide details about how you will track access to sensitive personal information.

BCNET

BCNET member institutions are responsible for ensuring that access to all personal information in their custody and/or control is secure, monitored and reviewed/audited on a regular basis.

Deem

Deem follows the PCI and SOC standards for logging and monitoring mechanisms. The company can track user activities that are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments (Windows systems, syslog config file on Linux systems and syslog for network infrastructure) and at the application level allows thorough tracking, alerting, and analysis when something does go wrong. Furthermore, Deem uses industry leading Splunk software to search, analyze and visualize the machine generated data gathered from various sources.

17. Describe the privacy risks for disclosure outside of Canada.

Use the table to indicate the privacy risks, potential impacts, likelihood of occurrence and level of privacy risk. For each privacy risk you identify describe a privacy risk response that is proportionate to the level of risk posed.

This may include reference to the measures to protect the sensitive personal information (contractual, technical, security, administrative and/or policy measures) you outlined. Add new rows if necessary.

Privacy risk	**Impact to individuals**	**Likelihood of unauthorized collection, use, disclosure or storage of the sensitive personal information (low, medium, high)**	**Level of privacy risk (low, medium, high, considering the impact and likelihood)**	**Risk response (this may include contractual mitigations, technical controls, and/or procedural and policy barriers)**	**Is there any outstanding risk? If yes, please describe.**
Unauthorized individuals at BCNET or member institutions could access personal information and use or disclose it for personal purposes.	High	Low	Medium	Employee Code of conduct and non-disclosure agreements, Use of Information & Technology Policies, password protected access, user access to system, based on need-to-know principles, permission	No

				restrictions, access controls, and monitoring.	
Unauthorized individuals at Deem could access personal information and use or disclose it for personal purposes.	High	Low	Medium	Information Security Policy which all employees must understand and adhere to. Annual independent information security reviews. Policies in place including Privacy Policy, Human Resource Security Policy, Physical and Environment Security Policy, Access Control Policy, Communication and Operations Management Policy	No
User's credit card number is compromised in Deem.	High	Low	Medium	Deem is compliant with the Payment Card Industry Data Security Standard Level 1. The standard encompasses all the IT and operational controls that organizations must implement to protect credit card data.	No

Inherent risk in Deem's use of third-party service providers	High	Low	Medium	All third parties and sub-contracted parties and their employees are required to adhere to Deem's Third-party Security Policy (ISP). Third parties are required to submit specified documentation pertaining to information security prior to any engagement. Service levels related to security are required to be monitored and reported by the relevant stakeholders. Third parties are subject to independent reviews of their compliance with the Deem ISP.	No
User's personal information is compromised during transmission	High	Low	Medium	Deem uses standard security protocols and mechanisms to exchange the transmission of sensitive data. When an individual enters sensitive	No

				personal information on the site, it is encrypted using Transport Layer Security (TLS) technology.	

Outcome of Part 4

The outcome of Part 4 will be **a risk-based decision made by the head of the public body on whether to proceed with the initiative**, with consideration of the risks and risk responses, including consideration of the outstanding risks in question 17. **The public body may document the decision in an appropriate format as determined by the head of the public body or by using this PIA template.**

PART 5: SECURITY OF PERSONAL INFORMATION

In Part 5 you will share information about the privacy aspect of securing personal information. People, organizations, or governments outside of your initiative should not be able to access the personal information you collect, use, store or disclose. You need to make sure that the personal information is safely secured in both physical and technical environments.

18. Does your initiative involve digital tools, databases, or information systems?

Yes.

- If yes, work with your Privacy Officer to determine whether you need a security assessment to ensure the initiative meets the reasonable security requirements of FOIPPA section 30

18.1 Do you or will you have a security assessment to help you ensure the initiative meets the security requirements of FOIPPA section 30?

No. Deem is compliant with the Payment Card Industry Data Security Standard Level 1.

- If yes, you may want to append the security assessment to this PIA. Go to question 20
- If no, go to question 19

19. What technical and physical security do you have in place to protect personal information?

BCNET

BCNET member institutions are responsible for ensuring the physical security of all data while in their custody and/or control (including data at rest or in transit) and must meet applicable physical security standards required by their organization.

BCNET member institutions are responsible for ensuring the technical security of all data in their custody and/or control (including data at rest or in transit) and must meet applicable technical security standards required by their organization.

Deem

The Deem Platform is separated into a web tier, application (or async) tier, and database tier. The tiers are formed by physically separate groups of servers and are separated by firewalls, load balancers or both.

Deem works with Cyxtera to provide secure, reliable, and scalable hosting services for their production environments. By combining a modern, hybrid-ready information Security fabric with an uncommonly diverse and distributed footprint of 57 world-class data centers and 3,500 customers, Cyxtera delivers a secure platform for connecting and protecting dedicated infrastructure, private clouds, and public clouds. All facilities are engineered to incorporate multiple levels of security and redundancy, ensuring maximum availability.

Utilizing physically separate facilities in Virginia, USA for their production data centers, Deem can safeguard valuable IT assets and data against manmade and natural disasters. The data center locations are designed to withstand extreme weather events and prevent unauthorized contacts from accessing the data center space. Data centers utilize power management, power monitoring, advanced fire suppression, and HVAC (heating, ventilation, and air conditioning) systems. To maintain power availability, the data centers utilize high capacity, redundant generators that guarantee power availability even during metro wide power outages.

20. Controlling and tracking access

BCNET members are responsible for controlling and tracking access to the personal information.

Strategy	
We only allow employees in certain roles access to information	Yes
Employees that need standing or recurring access to personal information must be approved by executive lead	Yes
We use audit logs to see who accesses a file and when	
Describe any additional controls:	Deem – access is based on least privilege and need-to-know principles. Deem follows the PCI and SOC standards for logging and monitoring mechanisms. The company can track user activities that are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments (Windows systems, syslog config file on Linux systems and syslog for network infrastructure) and at the application level allows thorough tracking, alerting, and analysis when something does go wrong. Furthermore, Deem uses industry leading Splunk software to search, analyze and visualize the machine generated data gathered from various sources.

PART 6: ACCURACY, CORRECTION AND RETENTION

In Part 6 you will demonstrate that you will make a reasonable effort to ensure the personal information that you have on file is accurate and complete.

21. How will you make sure that the personal information is accurate and complete?

FOIPPA section 28 states that a public body must make every reasonable effort to ensure that an individual's personal information is accurate and complete.

Individual users are responsible for ensuring the information in their user profile is accurate and up to date.

22. Requests for correction

FOIPPA gives an individual the right to request correction of errors or omissions to their personal information. You must have a process in place to respond to these requests.

22.1 Do you have a process in place to correct personal information?

Yes. Individuals can correct their own personal information through their profile.

22.2 Sometimes it's not possible to correct the personal information. FOIPPA requires that you make a note on the record about the request for correction if you're not able to correct the record itself. Will you document the request to correct or annotate the record?

N/A. See above.

22.3 If you receive a request for correction from an individual and you know you disclosed their personal information in the last year, FOIPPA requires you to notify the other public body or third party of the request for correction. Will you ensure that you conduct these notifications when necessary?

N/A. See above.

23. Does your initiative use personal information to make decisions that directly affect an individual?

No.

- If yes, go to question 25
- If no, skip ahead to Part 7

24. Do you have an information schedule in place related to personal information used to make a decision?

FOIPPA requires that public bodies keep personal information for a minimum of one year after it is used to make a decision. In addition, the Information Management Act requires that you dispose of government information only in accordance with an approved information schedule.

N/A

- If no, describe how you will ensure the information will be kept for a minimum of one year after it's used to make a decision that directly affects an individual.

PART 7: AGREEMENTS AND INFORMATION BANKS

Please provide information about whether your initiative will involve an information sharing agreement, research agreement or personal information bank.

25. Does your initiative involve an information sharing agreement?

No.

- If yes, please complete the Information Sharing Agreement Supplement and attach it to your PIA

26. Will your initiative result in a personal information bank?

A personal information bank (PIB) is a collection of personal information searchable by name or unique identifier.

No.

- If yes, please complete the table below.

Describe the type of information in the bank
Name of main organization involved
Any other ministries, agencies, public bodies, or organizations involved
Business contact title and phone number for person responsible for managing the PIB

PART 8: ADDITIONAL RISKS

Part 8 asks that you reflect on the risks to personal information in your initiative and list any risks that have not already been addressed by the questions in the template.

27. Risk response

Describe any additional risks that arise from collecting, using, storing, accessing or disclosing personal information in your initiative that have not been addressed by the questions on the template.

See #17 for Privacy Risks

Possible risk	Response

PART 9: SIGNATURES

You have completed a PIA. Submit the PIA to your Privacy Officer for review and comment, and then have the PIA signed by those responsible for the initiative.

Privacy Office Comments

Privacy Office Signatures

This PIA is based on a review of the material provided to the Privacy Office as of the date below.

Role	Name	Signature	Date signed
Privacy Consultant	Bev Hooper, Hooper Access and Privacy Consulting Ltd.		Jan 12/22

Program Area Signatures

This PIA accurately documents the data elements and information flow at the time of signing. If there are any changes to the overall initiative, including to the way personal information is collected, used, stored, or disclosed, the program area will engage with their Privacy Office and if necessary, complete a PIA update.

Program Area Comments:

Role	Name	Signature	Date signed
Initiative lead			
Program/Department Manager	Dennis Silva, Chief Procurement Officer		2022-01-14
Contact Responsible for Systems Maintenance and/or Security Only required if they have been involved in the PIA			
Head of public body, or designate Only required if personal information is involved	Bala Kathiresan President and Chief Executive Officer		Jan. 14, 2022

Deem PIA - Final

Final Audit Report 2022-01-14

Created:	2022-01-14
By:	Trisha Rana (trisha.rana@bc.net)
Status:	Signed
Transaction ID:	CBJCHBCAABAAXzQM5sRn57r0NdHfmvtcL6x4G8pnk8N9

"Deem PIA - Final" History

Document created by Trisha Rana (trisha.rana@bc.net)

2022-01-14 - 8:06:29 PM GMT- IP address: 142.231.1.180

Document emailed to Dennis Silva (dennis.silva@bc.net) for signature

2022-01-14 - 8:08:34 PM GMT

Email viewed by Dennis Silva (dennis.silva@bc.net)

2022-01-14 - 9:41:55 PM GMT- IP address: 104.47.61.254

Document e-signed by Dennis Silva (dennis.silva@bc.net)

Signature Date: 2022-01-14 - 9:42:57 PM GMT - Time Source: server- IP address: 142.231.1.177

Document emailed to Bala Kathiresan (bala.kathiresan@bc.net) for signature

2022-01-14 - 9:42:59 PM GMT

Email viewed by Bala Kathiresan (bala.kathiresan@bc.net)

2022-01-14 - 10:04:17 PM GMT- IP address: 104.47.61.254

Document e-signed by Bala Kathiresan (bala.kathiresan@bc.net)

Signature Date: 2022-01-14 - 10:06:30 PM GMT - Time Source: server- IP address: 142.231.1.177

Agreement completed.

2022-01-14 - 10:06:30 PM GMT