



General Data Protection and Regulation (GDPR) Compliance

Policy and Procedure Handbook

Version A

May 21, 2018

Send Questions to
Privacy@Seattle-C.com

1. Introduction
 - 1.1 Purpose
 - 1.2 Scope
 - 1.5 Employee Privacy Training Programs
 - 1.6 Record of Processing Activities
 - 1.7 References
2. Data Privacy Policies
 - 2.1 Data Flow
 - 2.1.1 Individual data
 - 2.1.2 3rd Party Data Overlay
 - 2.1.3 Ad Platforms
 - 2.1.4 Impact Analytics
 - 2.1.5 Merchandising optimization
 - 2.1.6 Offline Segmentation
 - 2.2 Data Flow Across Data Centers
 - 2.3. Privacy Policy - Data Collection
 - 2.3.3 Repurposing the data
 - 2.3.4 Notifying the user
 - 2.3.5 Data Protection Impact Assessment (DPIA)
 - 2.4 Data Retention Policy
 - 2.4.1. Data Storage
 - 2.4.2 Retention Period
3. Data Breach Handling Policy
 - 3.1 Reporting a Data Breach Incident
 - 3.2 Data Breach Classifications and Mitigation Plan
 - 3.3 User Notification
 - 3.4 Escalation Process
 - 3.5 Breach Log Maintenance and Notifications
 - 3.6 Test Plan and Review
 - 3.7 Data Breach Incident Management Team
- 4 Disaster Recovery Plan
 - 4.1 User Notifications

4.2 Data Recovery Plan

4.3 Data Backup

4.4 Test and Review

4.5 Disaster Recovery Management Team

1. Introduction

Seattle-C has built a platform that ensures all industry standard privacy regulations are met. A comprehensive analysis of the company's present data privacy and protection policies and processes have been carried out; including analysis of how data is collected, used and shared by Seattle-C platform.

Seattle-C is also working with all the partners, clients and vendors to ensure they all fulfil their GDPR compliance obligations. Seattle-C privacy policy and data privacy practices have been reviewed and contractual provisions with the partners, clients and vendors have been put in place.

1.1 Purpose

This document is a single point of reference for all the processes and procedures that are being followed at Seattle-C to remain GDPR compliant. This is a living document and the policies mentioned in this document will be reviewed and updated by the Seattle-C privacy team on a need basis.

1.2 Scope

This document is for all interested parties internal and external to Seattle-C who would like to know about the GDPR compliance related guidelines that are being followed at Seattle-C. This document can be used for Audit purposes. Each section of this document describes the various aspects of customer data privacy policies and procedures that are being adhered at Seattle-C. Additional information can be found in the supporting documents mentioned in the references section.

1.5 Employee Privacy Training Programs

To protect the privacy of the customers/users, it has been ensured that all Seattle-C employees understand the importance, Dos and Don't of how data should be handled. A comprehensive training program has been developed and it is mandatory for all new and old employees to undergo this training. The entire training can be found [here](#). The training completion log can be found [here](#).

1.6 Record of Processing Activities

A process is in place to assess the *Record of Processing* document at Seattle-C. The current Record of Processing for Consumers and Vendors can be found [here](#).

This document will be updated annually and the following process is in place to do so:

1. Jira automatically creates a Reminder ticket on May 1 with a due date of May 31 to review and update the Record of Processing. The ticket is assigned to "privacy" to review the Record of Processing.
2. Everyone on the "privacy" alias will get an email notification when the ticket is created. All reminder tickets will roll up into [PM-572](#) so that a dashboard can be easily created or put the Jira status on a Confluence page.

This method is automated. A Jira ticket is generated annually and assigned to mailing lists so that the right teams get notified. It is set up using the "Recurring Tasks" plugin for Jira.

1.7 References

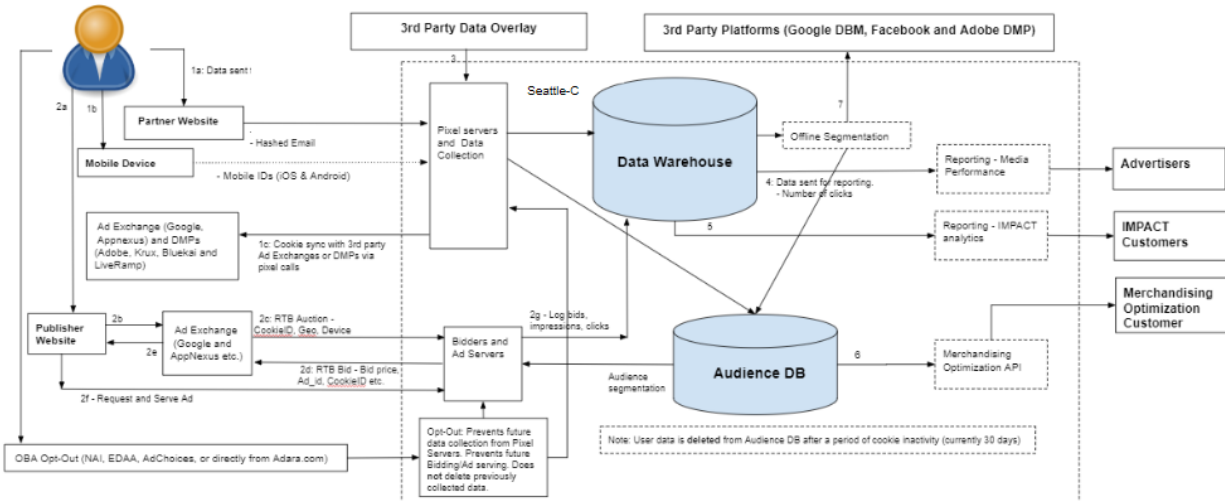
Find below a list of articles in support of the information provided in this document.

<i>Document</i>	<i>Description</i>
Seattle-C Privacy Policy Notice	Available for the users to review at www.Seattle-C.com
Initial Screening Assessment (ISA)	Template to perform ISA for all Seattle-C products
Data Protection Impact Assessment (DPIA)	Template to perform DPIA for all Seattle-C products

2. Data Privacy Policies

2.1 Data Flow

The below diagram describes how various types of data is collected through different sources/channels and methods - stored, used for analytic purposes and deleted from the system.



2.1.1 Individual data

Data from individual users gets into the Seattle-C system through the following channels:

- Flow #1a:** Partner pixel integration: User visits a partner website and Seattle-C pixel fires. Data is saved in Seattle-C Data warehouse and Real time audience DB. Seattle-C also fires 3rd party pixels to sync CookieID with Ad Exchanges, Publishers, and DMPs. Google also fires their ID to sync with Seattle-C.
- Flow #1b:** Mobile Device: Mobile ID is received through the Mobile Device. However, not all partners send Mobile information.
- Flow #2:** RTB Media flow: User visits a publisher website. Ad Exchange on the site will conduct RTB auctions with bidders including Seattle-C. Seattle-C responds with a bid, using data previously collected on the user to inform the bid. If auction is won, Seattle-C will serve the Ad. Bids, impressions, and clicks are logged for the user. However, does not apply to 3rd party platforms in which Seattle-C does not control the bidding and/or Ad serving process.

2.1.2 3rd Party Data Overlay

Flow #3: DMP sends data to Seattle-C, keyed by previously synced cookies from Flow #1, for e.g.; Adobe, Bluekai, Krux and LiveRamp etc. Seattle-C saves this data in the Data Warehouse and Audience DB for future Ad targeting.

2.1.3 Ad Platforms

Flow #4: Media Reporting: Seattle-C summarizes raw advertising events (Bids, Impressions and Clicks) into higher level reporting metrics. The reports are delivered to Advertisers via UIs or CSV file downloads.

2.1.4 Impact Analytics

Flow #5: Seattle-C generates analytics using data collected through Flow #1, #2 and #3. The analytics are delivered to customers via Seattle-C UIs.

2.1.5 Merchandising optimization

Flow #6: Merchandising optimization. Derived signals for eg.; “seat upgrade propensity” for airlines can be queried by Customer via API for use in their booking engine. The data would be looked up based on common UserID like Hashed Email address.

2.1.6 Offline Segmentation

Flow #7: Pushing segments to 3rd Party Platforms - Google DBM, Facebook and Adobe DMP. This may contain UserID and key values like Geo, Date etc. for managed campaigns run by Seattle-C.

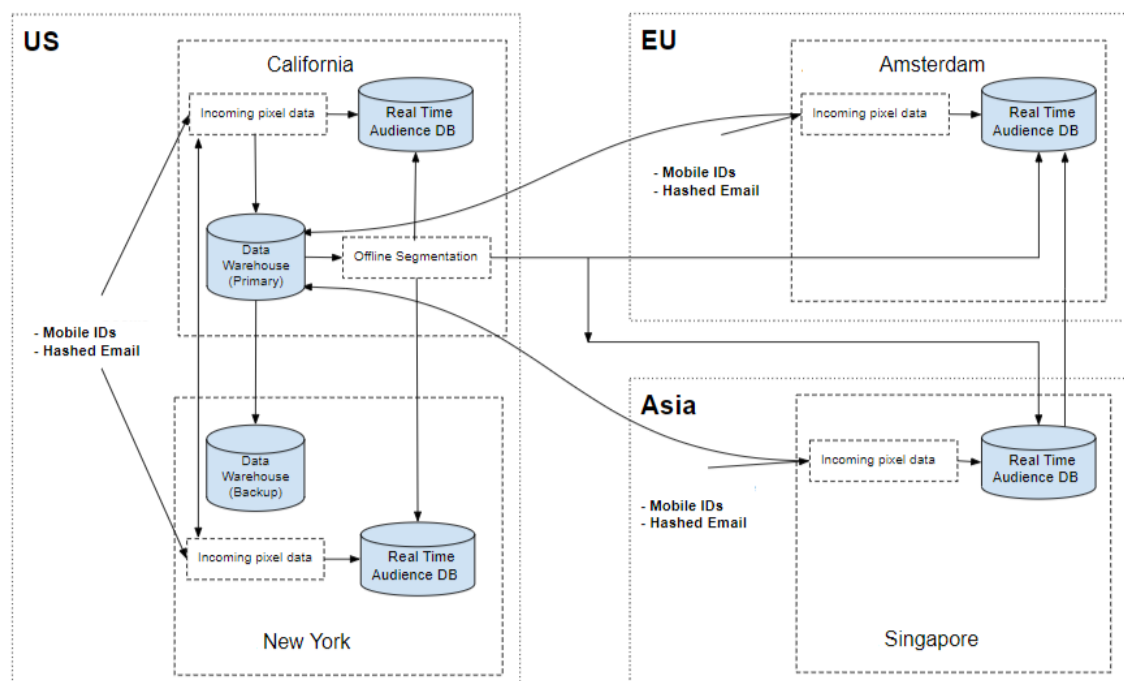
2.2 Data Flow Across Data Centers

Seattle-C receives incoming pixel data from various sources, which may contain EU data in all four Data centers located across the globe: *United States, Netherlands and Singapore*.

Data from all locations are being sent to and processed by the Data Warehouse located in the US. Offline Segmentation processes are run in US, and the output of those can be distributed globally to all data centers, and used for the following purposes:

- RTB media campaigns
- Non-RTB media campaigns (shared with external platform like Google DBM)
- Shared with Merchandising Optimization API customers

The below data flow map shows the details:



2.3. Privacy Policy - Data Collection

Data is collected through different channels as mentioned above in [section 2.1](#) and are being used to create solutions for Seattle-C partners. Data is collected only from those users who have provided their consent in the partner websites. Refer to Seattle-C Privacy Policy Notice at <https://Seattle-C.com> for additional information.

2.3.3 Repurposing the data

Seattle-C collects the data, and then decides on the specific business use depending on one of the three main business activities in the travel ecosystem:

Online advertising: The collected data will be used to make decisions or buy, monitor, or report on the delivery of online advertising for our advertiser via Ad exchanges. The performance data may be also shared with advertisers and their representatives in the digital advertising ecosystem. During this process, Seattle-C may overlay third-party data collected from third-parties, in order to enhance the decision making.

Measurement and Analytics: Once Seattle-C collects data, it is collated and classified in the database in aggregated form, and may be made available via reporting or via the Seattle-C platform for high level trend analysis in an aggregated form. Data is also used to create analytics about travel industry trends, effectiveness of media, or for content marketing.

Traveler Intelligence: Seattle-C may share aggregated, pseudonymous data with its partners or clients for the purposes of enhancing their CRM for personalization or merchandising optimization.

The collected data may also be transferred either in aggregated or collected format to the cloud data centers or hosting providers. The data will also be used for specific internal Seattle-C operations including troubleshooting, data analysis, testing, research, and statistical or survey purposes.

Seattle-C will limit the use of personal data so that it is consistent with the disclosures and consent provided.

2.3.4 Notifying the user

Seattle-C does not collect data directly from individuals. Data is shared by the partners, clients and vendors. Seattle-C will review and make necessary updates to the privacy policy, contracts and data privacy practices to ensure the subjects are aware of the processing.

2.3.5 Data Protection Impact Assessment (DPIA)

The DPIA is a mandatory process required by the [EU Data Protection Regulation](#) (GDPR).

Prior to new products being available to customers, an Initial Screening Assessment (ISA) and potentially a Data Protection Impact Assessment (DPIA) must be completed.

1. Initial Screening Assessment (ISA) - must be completed for all NEW product offerings.

Answering "yes" to one or more questions indicates a DPIA may be needed.

A [template](#) is available for all Product Managers to use and carry out the assessment.

The following ISAs are available for current products at Seattle-C:

- [ISA for AppsFlyer](#)
- [ISA for Data Activation Services](#)
- [ISA for Data Partners / Data Monetization](#)
- [ISA for Digital Media](#)
- [ISA for ichnaea \(Internal Tool for Magellan\)](#)
- [ISA for Impact](#)

2. Data Protection Impact Assessment (DPIA)

- a. Required for ISA assessments that have "yes" to one or more questions mentioned above
- b. Required for products that will have a change to how data is collected, stored, used, or deleted

3. For any action items as a result of the DPIA, create a Jira ticket (with Epic = GDPR: ENG-1782) which will be tracked on this page: [Data Protection Impact Assessment \(DPIA\)](#)

A [template](#) is available for the assessment. The following DPIAs are available for current products:

- [DPIA for Seattle-C.com \(includes Google Analytics\)](#)
- [DPIA for comScore and Amobee \(Turn Inc.\)](#)
- [DPIA for Data Activation Services](#)
- [DPIA for Data Partners / Data Monetization](#)
- [DPIA for Digital Media](#)
 - [DPIA for Ichnaea \(Internal tool for Magellan\)](#)
- [DPIA for ID Graph](#)
- [DPIA for IMPACT](#)
- [DPIA for Pendo \(3rd party tool for Impact and Magellan\)](#)
- [DPIA for Salesforce](#)

2.4 Data Retention Policy

Seattle-C collects user data from Partner Websites, Mobile Devices and Publisher Websites as mentioned in [section 2.1](#) above. Data will be retained in the Audience Database in the form of Cookies. Collected data is stored in the internal databases which are cloud based systems.

2.4.1. Data Storage

Data is stored in the four data centers as mentioned in [section 2.2](#). The data center locations are: United States, Netherlands and Singapore. These data centers are provided by 3rd party AppNexus, AWS and Google Cloud Platform.

2.4.2 Retention Period

Data retention policy in Seattle-C is as follows:

- Data in the Data Warehouse will be retained for 2 years for analytic purposes.
- If a cookie in the Audience DB is inactive for 30 days it will be archived automatically.
- For online identifiers like Mobile IDs that remain active indefinitely for the use of the device, Seattle-C will dissociate the data after the period of 2 years from last encounter.
- In addition, Seattle-C will retain the respective sets of information received through the Partner websites or the Seattle-C website for as long as needed to fulfill a legitimate business need. Necessary information is used and retained to comply with the legal obligations and to enforce any agreements.
- For users who have Opted-out and do not want to receive any marketing communication/advertising from Seattle-C or any of the partners, those users will be flagged as Opted-out and their data will not be used for any future campaigns. However, historical data will be archived in the database.

3. Data Breach Handling Policy

This section provides a high-level guideline and general policy of all of the requirements and procedures necessary in order to facilitate quick response, mitigation, and communication in the event of a data breach. This is to ensure that all policies, procedures, and best-practices are in place and also properly communicated, such that preventative and corrective measures that are put in place for the mitigation of data breaches are effective and comply with global privacy laws and policies. Data Breach Mitigation activities must adhere to the policies and recommendations set forth in this document.

3.1 Reporting a Data Breach Incident

A data breach incident can be reported to the Seattle-C team by any of the partners/vendors or Seattle-C employees by sending an email to Privacy@Seattle-C.com. Seattle-C Data Protection Officer (DPO) - Angela Sultana is informed and an investigation is initiated.

Seattle-C has a dedicated Operations team who manages all the data breach incidents. Incidents can be reported to the Operations team through Seattle-C Products support teams as well.

3.2 Data Breach Classifications and Mitigation Plan

Data breaches typically fall into two different classes:

1. Class I: Data breach that involves legally protected information
 - Customer or Employee personally identifiable information accessed or otherwise made available to unauthorized entities.
2. Class II: Data breach that represents material loss to the company
 - Source code or other materially important, documentation containing proprietary or otherwise confidential information; the loss of which or access by unauthorized entities, compromises, disrupts or otherwise impairs the company's ability to maintain business continuity.

There are various ways in which a data breach may happen. Below are some example scenarios that are considered breach incidents that need mitigation response.

Scenario	What is at risk?	Data Breach Classification	Mitigation	Responsible Parties
Lost/Stolen Employee Laptop	Employee access credentials <ul style="list-style-type: none"> ● All: proprietary documentation ● Dev: source code ● Dev: database 	Potential Class I	<ul style="list-style-type: none"> ● All Employee Laptops are secured by login credentials ● Remote-wipe capability enabled on employee 	<ul style="list-style-type: none"> ● IT/Desktop Support ● Production Operations ● HR

	access (customer emails) <ul style="list-style-type: none"> • HR: employee information • F&A: Financial information, employee information 		laptops NOTE: This item is in-progress and the IT team is working towards completing it in all employee laptops. JIRA ticket #ENG-2018 <ul style="list-style-type: none"> • Access credentials can be removed and disabled across the board 	
Corporate Network Intrusion	<ul style="list-style-type: none"> • Employee personal information • Company financial information 	Potential Class I	<ul style="list-style-type: none"> • Corporate Network resources are protected by access credentials • User laptops run antivirus software to detect malicious activity 	<ul style="list-style-type: none"> • IT/Desktop Support • HR • Finance & Accounting
Production Network Intrusion	<ul style="list-style-type: none"> • Customer emails and encrypted passwords (customer emails) • Potentially personally identifiable information such as encrypted email and cookie IDs • Hosted infrastructure is at risk if business is disrupted by malicious unauthorized access 	Potential Class I or Class II if network is maliciously compromised to impair business-continuity	<ul style="list-style-type: none"> • Access is secured following industry best-practices and guidelines • Systems are monitored for intrusion detection • Personally identifiable data is encrypted, thereby limiting usefulness of data in the event that it's accessed by unauthorized parties 	Production Operations

3.3 User Notification

A **Class I** data breach requires that the victims of the breach are notified. The following outlines the steps to go through in order to properly communicate a breach effectively. These procedures are in place both to clearly communicate risks to data breach victims, as well as minimize the damages to company business continuity.

1. Once a data breach has been identified as a **Class I** breach, the mitigation team will escalate to the *Data Privacy Team* at privacy@Seattle-C.com
2. The *Data Privacy Team* shall consult with legal counsel and relevant mitigation teams (i.e. ProdOps or HR or IT/Desktop support) to craft a comprehensive response.
3. The crafted response will be sent out to the relevant *Communications Team(s)* by DPO Angela Sultana for wider distribution to the affected parties.

Once investigated and confirmed that there has been a data breach incident the **Information Controller's Office (ICO)** will be notified within 24 hours of fact finding. The following information will be shared in the notification:

- Seattle-C DPO name and contact details
- The date and time of the breach (or an estimate)
- The date and time when Seattle-C detected it
- Basic information about the type of breach
- Basic information about the personal data concerned

The [breach notification form](#) will be used to notify ICO.

3.4 Escalation Process

Once the operations team is notified of any Data Breach incident, the following process will be followed to escalate it to the concerned team.

1. One of the operations team engineers will be on-call 24x7 each week. The rotation will start on Tuesday 10am and will end at 10am on following Tuesday.
2. Once an on-call engineer is notified of a data breach incident the below mentioned process will be followed:
 - a. Immediately a JIRA ticket will be created, under - **Operations->Incident (Component: Data Breach)**
 - b. The impact of the problem will be determined such as Who or What business activities does it affect?
 - c. Based on the scope and impact, relevant fields of the incident report will be filled in the JIRA ticket and notifications will be sent out.

3.5 Breach Log Maintenance and Notifications


As mentioned in [section 3.4](#), a JIRA ticket is created to track all data breach incidents. An automated internal breach incident log register which is connected to JIRA is created and maintained, available [here](#).

Automatic Email notification of active data breach incidents in JIRA is sent every **2 hours** to the internal Seattle-C GDPR group list maintained in JIRA/Confluence. This list includes team members from both Engineering and Privacy teams. A sample notification is shown below:

[JIRA] Subscription: Notification: Active Data Breach Reported Inbox x

jira@adara-inc.atlassian.net 12:40 PM (22 minutes ago) ★
to me ▾

Issue Subscription
Filter: [Notification: Active Data Breach Reported \(1 issue\)](#)
Notification that there is an Open Incident involving a Data Breach
Subscriber: karen.woodmansee

T	Key	Status	Incident Start Time	Summary	Nature of Breach
 Incident	OPS-778	NEW	02/Apr/18 11:16 AM	Karen TESTING new fields for Data Breach -- IGNORE	


You may edit this subscription [here](#).

In case of missing data or fields in the already Resolved data breach incidents tickets, a Reminder email notification is sent out daily to the team to keep the log accurate and up to date. A sample notification is shown below:

[JIRA] Subscription: REMINDER: Fill in missing fields for Resolved Data Breach Inbox x

jira@adara-inc.atlassian.net 12:53 PM (18 minutes ago) ★
to me ▾

Issue Subscription
Filter: [REMINDER: Fill in missing fields for Resolved Data Breach \(1 issue\)](#)
Reminder to update "Notified?" field to Yes/NotNeeded and to fill in fields on the "Data Breach Details" tab
Subscriber: karen.woodmansee

T	Key	Summary	Notified?	Number People Affected	Nature of Breach	How Breach Surfaced	Description of Data	Consequences of Breach	Remedial Action	Other Regulators Informed	Date ICO Notified
 Incident	OPS-778	Karen TESTING new fields for Data Breach -- IGNORE	No		Disclosed in error	Realized when..	excel file containing link	test env pwd sent to home address	Pwd reset on test env		02/Apr/18

3.6 Test Plan and Review

As part of the annual review of the Data Breach Mitigation Plan, portions of the plan, specifically those pertaining to preventative measures and key security policies will be reviewed, audited, and otherwise exercised as necessary. The exercising of the Data Breach Mitigation Plan components ensures the validity, and effectiveness of it on a regular basis. Therefore, the Data

Breach Mitigation Plan will be reviewed once per calendar year and the following measures will be taken:

- Review Employee Security Policies
 - Password strength, complexity and periodic changes
 - Securing employee equipment
 - Identifying and avoiding phishing or socially-engineered attacks
- Assess corporate network health
 - Penetration test
 - Audit user access logs
- Assess production network health
 - Penetration test (periodically monitored in real-time)
 - Audit access logs (monitored in real-time)
- Review regional privacy laws and ensure this document complies with the requirements outlined in those laws
 - Privacy Team will work with legal counsel to do an annual review

3.7 Data Breach Incident Management Team

An operations engineer is on-call 24x7 to attend all alerts via Email or Phone. Any data breach issue will be escalated to the team immediately. Below mentioned is the internal team and their contact details:

Key Personnel Contact Information

Team	Location	Name	Phone/Email
Production Operations Primary	Seattle	operations@Seattle-C.com ops-pager@Seattle-C.com (emergency pager)	(408) 472-9959
Production Operations Secondary			(408) 472-9087
HR	Seattle	Leslie	Leslie.Hooper@Seattle-C.com
Privacy	Chicago	Angela	(773) 817-XXXX

Data Breach Mitigation Team

Role	Team	Responsible Party
Data Breach Assessment	Production Operations	Dylan

	Data Integrity	Jian
Data Breach Mitigation	Production Operations	Dylan
	Desktop Support/IT	Rhino Support

4 Disaster Recovery Plan

A disaster recovery plan is in place at Seattle-C which describes the requirements and procedures necessary in order to facilitate a quick and error-free recovery of business-continuity when faced with disruptive failure conditions in the production environment. This section describes the procedures that will be followed to secure the data and notify the users/customers in such situations.

4.1 User Notifications

Once an issue is identified, and it is established that there is a potential breach to data privacy, all partners, vendors and data providers will be notified and communicated by the Seattle-C Privacy team. The ICO will be notified as mentioned in [section 3.3](#).

4.2 Data Recovery Plan

The on-call operations engineer will identify the severity of the issue and notify the key members as mentioned in [section 3.7](#) through the prod-issue@Seattle-C.com alias.

Issue will be escalated to the Production Manager and if unable to resolve in 30 to 45 mins, data recovery will be initiated from the backups by the Operations team.

4.3 Data Backup

Seattle-C does real time backup of the business continuity data in Google Cloud Platform. All storage and backups are automated. For Data Encryption, backups are 2048 - bit RSA and warehousing are AES-256.

4.4 Test and Review

As part of the annual review of the Disaster Recovery Plan, portions of the plan, specifically those pertaining to readiness and backup, prevention, and preparative activities performed in support of the Disaster Recovery Plan, will be reviewed, audited, and otherwise exercised as necessary. The exercising of the Disaster Recovery Plan components ensures the validity,

effectiveness, and continued relevance of this section on a regular basis. The Disaster recovery plan will be reviewed at least once per calendar year along with the below system verifications:

- Verify that all database backups are current and available
- Verify that source control backups are current and available
- Verify that BDB backups are current and available
- Verify that current base OS images are available on distributed storage
- Verify that current software is available on distributed storage
- Verify that Jenkins build configuration backup is current and available

4.5 Disaster Recovery Management Team

The key team members are mentioned in [section 3.7](#) . They will be contacted for guidance and notified in case of any emergency. The below team members are responsible to mitigate the issue.

Disaster Recovery Team

Role	Team	Responsible Party
Disaster Recovery	Production Operations	Dylan
Infra Vendor Communications	Production Operations	Dylan
Vendor Communications	Product Team, Ad Ops	Nikhil Karla