Data Enablement Plan (DEP) Program Playbook

Data & Trust Office

2023

Introduction

The purpose of this document is to provide a comprehensive overview of the Data Enablement Plan (DEP) Program, including information on process workflows, roles and responsibilities of key stakeholders, and critical applications.

Data Enablement Plan - Program Overview

The Data Enablement Plan (DEP) program supports the identification of risk and enablement of responsible data use for TELUS using a technology enabled platform. By unifying our Privacy Impact Assessment (PIA) and Secure by Design (SbD) review into a single process, we are improving our agility through data stewardship, supported and led by the Data & Trust Office (DTO) and the Corporate Security Office (CSO).

Key features and benefits include:

1. A unified experience and a streamlined questionnaire.
2. Integration of risk identification to ensure risks are identified early in a project life-cycle.
3. Agile and timely review.
4. Trained Data Steward designated to a business to support the submission of a DEP.
5. Technology-enabled, user-friendly tool, that allows for transparency and accountability.

Data Stewardship

Role

Data Stewards are TELUS team members appointed by their executive to take on a leadership role in the business unit for responsible data use in collaboration with the Data & Trust Office and Chief Security Office teams. Data Stewards have intimate knowledge of the day-to-day intended data use cases and understand the intended business strategy of the data initiatives within their respective business unit. They have a critical role in enabling the use of data in their area of the business by driving Data Enablement Plans (DEP). Data Stewards work with their team to support data risk mitigation and monitoring activities as new initiatives are launched. Certified Data Stewards have the ability to determine and sign off no data risk sections.

Responsibilities of a Data Steward

1. Work with their business unit to submit DEP assessments and connect with the applicable Subject Matter Experts for DEP consultation/review.

2. Support the identification of any applicable data risks or mitigating tasks, and prepare the DEP for approval by the applicable Executive.
3. Monitor the completion of any tasks identified in the DEP and mark the plan as 'Complete' to ensure the business is ready to launch their new initiative.

Data Steward Enrollment and Training

Data Stewards may be appointed by their leadership team, nominated by their business unit, or may self-enroll with the approval of their leadership team. Team members can enroll via the Data Steward Enrollment form, which can also be accessed through go/datasteward. Once enrolled, the DEP program manager will on-board the Data Steward using the "Data Stewards Onboarding" checklist.

Data Stewards are required to complete 3 foundational courses in Google Classroom (access will be provided after your enrollment) and will be given access to the OneTrust Lab environment (non-production) to become familiar with the DEP submission and completion process.

Once training is completed, Data Steward profiles are moved from the OneTrust Lab environment into the relevant organization/product portfolio module, which allows data stewards to begin submitting DEPs on behalf of their organization or portfolio. Level 1 certification is granted when three DEPs are completed.

Data Stewardship Support

There are several mediums of support available for Data Stewards:

- Peer to peer partnerships (Buddy program)
- Course based labs
- Data Steward office hours
- DEP|DS Job Aid
- Resources for Data Stewards
- Data Steward forum (monthly)
- Dedicated group Google Chat and Slack Channel
- Google Classroom (courses and videos)
- go/DEP Habitat resource page

Leaving the Data Stewardship Program

It is the responsibility of the Data Steward to advise the DEP program manager that they are leaving the Data Steward role, and to provide a suitable replacement. To offboard from the role, the Data Steward is expected to complete the offboarding section of the Data Steward Insight Form.

DEP Deputies

Role

A DEP Deputy helps the Data Steward answer the DEP questionnaire and provides supporting documentation where required. A deputy can be a project manager, a technical Subject Matter Expert (SME), or anyone on a project team that can help provide more clarity on an initiative.

Responsibilities of a Deputy

1. Support the Data Steward in answering the DEP questionnaire and providing supporting documents where required.
2. Complete the DEP Deputy Training, which provides insight into roles and navigation of the DEP.
3. Complete the attestation.

Deputy Enrollment and Training

Deputies are subject matters experts embedded in the business area. Data Stewards can leverage their expertise to ensure DEP questions are being answered as accurately as possible. To have a team member available as a Deputy, the Data Steward must direct them to the training and form available from go/DEP.

Note: Deputies cannot submit the DEP questionnaire, the Data Steward is responsible for the submission of the DEP.

Deputy Support

There are several mediums of support available for Deputies:

- Training and form available from go/DEP
- DEP Deputy Training
- Attestation

DEP Subject Matter Experts

Role

DEP Subject Matter Experts (SMEs) within the Security and Privacy offices provide guidance to data stewards on risks identified within the DEP.

Important things to remember:

- The DEP is a “plan” and will identify the potential risks and tasks required to be completed as part of enabling data.
- HIVE can be triggered to discuss uncertainties with the DEP. HIVE brings together key team members to work collaboratively to ensure a successful resolution to the DEP. Each HIVE is made up of a set of complementary skills that are needed for a successful project delivery.

Responsibilities of a SME

1. Providing support to the Data Steward in their respective areas of expertise.
2. Identifying tasks to be completed as part of the DEP.
3. Data Risk management.

SME Onboarding and Training

SMEs are provided with training on their role and on using OneTrust. Training documentation is available at go/DEP123. Training includes the following subjects:

1. DEP and Process Overview.
2. OneTrust Navigation.
3. Data Risk Management.
4. OneTrust Lab.

SME Support

There are several mediums of support available for DEP SMEs:

- Peer to peer partnerships (assigned buddies)
- DEP SME office hours (weekly)
- DEP|DEP SME Job Aid
- Dedicated Google Chat
- go/DEP123
- go/DTOPartnerTraining

DEP Director approval

Role

DEPs must be approved by the sponsoring Director before implementation of the roadmap and subsequent launch of the new initiative.

Responsibilities of a Director in DEP approval

1. Director will receive an email from OneTrust or the Data Steward will contact them and provide the link to the DEP for approval.
2. The link will prompt the director to sign into the DEP platform at https://telus.my.onetrust.com or go/onetrust; director enters TELUS email address.
3. Director navigates the DEP to review the assessment responses to ensure accuracy; and review the required tasks to understand the roadmap to enable the initiative.
4. Select 'Finish Review' and choose 'Approved' or indicate otherwise.

Director Support

There are several mediums of support available for Directors:

- Director Approval Instructions Quick Reference
- Director Approval of the DEP Job Aid

HIVE

What is HIVE?

HIVE is held with the purpose of providing an agile forum for various DTO and CSO SMEs to bring up questions regarding a specific DEP.

HIVE aids in accomplishing many tasks, including:

- Acting as a collaborative session;
- Streamlining a single meeting with various SMEs on the same topic; and
- Prompting proactive discussion around potential data risks or areas of uncertainty within a DEP.

Who will be at HIVE?

At HIVE, you will be able to chat with specific data risk management experts from the Data & Trust Office (DTO) and the Chief Security Office (CSO).

What is the HIVE process?

Data Stewards may be required to attend HIVE. After reviewing the DEP, DEP SMEs , including the Data & Trust partner (Privacy) and the Secure by Design partner (Security), may ask the data steward to schedule a HIVE. Any business SMEs that have essential knowledge about the initiative should be invited by the Data Steward. Please do not invite vendors to HIVE without first discussing with your DEP SMEs.

If a HIVE session is necessary, a DEP SME will generate an "Info Request" on the DEP with detailed instructions on how to schedule the session.

Access Requirements

Team members must complete training prior to being granted access to the OneTrust platform. There are three types of roles for the DEP, each requiring their own training as outlined in the sections above:

- Data Steward
- Deputy
- DEP SME

The Data Stewardship program manager collaborates with the OneTrust administrator to ensure users are being granted access in a timely manner.

In the case that an external user (i.e. consultant) requires access to the OneTrust platform, the project manager must connect with the Data Stewardship program manager to discuss the access requirements. The Data Stewardship manager collaborates with the OneTrust administrator to identify potential risks and obtain sign off from Privacy and/or Security if needed.

External user access to OneTrust

In the case that an end-user with a non-TELUS email domain requires access to OneTrust, the end-user must submit a Request for Change ticket via OneTrust. Upon approval from the Data Governance director, the individual must follow the appropriate onboarding path and complete training as required. The end-user will then be granted access to the OneTrust platform with the requested user role.

Program Communications

The following communication channels are currently in place for the DEP:

Data Stewards

- Monthly forums, google chat, go/dep

DEP SMEs (CSO/DTO)

- Weekly office hours

Business

- go/datasteward

Executive

- Executive data council

OneTrust Administration

Adding Data Stewards

The Data Steward manager manages the “Data Stewards Onboarding” tracking document. This tracker is used to notify the OT administrator when users need to be added to the platform or if their role needs to be modified.
The administrator is responsible for creating a user account for the team member in OneTrust. The user role will depend on what is specified in the onboarding process document.

Adding Deputies

The OneTrust administrator is notified via the Google registration form. The administrator should subscribe to receive email notifications from this form.
The administrator is responsible for creating a user account for the team member in OneTrust.

Adding Directors

Director names are bulk uploaded to OneTrust when a new business unit or organization is onboarded into the DEP process. Ad-hoc requests to add director names can also come through Google Chat or email.

Feedback

The following tools are available to Data Stewards to provide feedback to the DTO:

- Data Steward Insight Form
- go/depfeedback
- Data Steward Communication Channels (google workspace)
- DTO DEP SME Support Communication Channel (google workspace)

Appendix A - Key Contacts

- Data Steward manager - Laura Lawton
- DEP program manager - Rohin Bansal
- OneTrust administrator - Juan Arango
- OneTrust governance - Karen Clarke
- HIVE coordinator - Julie McGranachan

Appendix B - OneTrust

Logging into OneTrust

1. Go to https://telus.my.onetrust.com/ or go/onetrust.
2. At the login screen, enter your TELUS email address.
3. Click ‘Next’. (Please DO NOT click ‘Forgot Your Password’ since we use SSO)
4. You may need to enter your smart card password.

Note: OneTrust uses SSO (Single Sign-on). Users should not click ‘Forgot Your Password’ on the sign-in screen

Appendix C - Reports

The DTO team keeps track of the following DEP related metrics:

- Risk Level by ELT
- Managed Risks
- Risks without and Assignee
- Total Number of Risks
- Open DEP Tasks
- Risks with Open Tasks
- Number of DEPs by organization
- Accepted Risks
- Mitigated vs Accepted Risks

These dashboards can be found in OneTrust. The DTO manages access to the dashboards.

Appendix D - Resources

- Data Stewardship (go site)
- DEP|DS Job Aid
- Resources for Data Stewards
- DEP training (Google Classroom)
- Data Steward Enrollment Form
- Data Risk Management Policy
- Data Risk Management Framework
- Data Steward Mandate
- DEP123
- go/dtopartnertraining
- go/dep
- go/dto

- go/datarisk
- go/privacy
- OneTrust
- TELUS Data Governance
- DEP Deputy Training
- Deputy attestation
- DEP|DEP SME Job Aid
- Director Approval Instructions Quick Reference
- Director Approval of the DEP Job Aid

Appendix E - Glossary

- DS - Data Steward
- DEP - Data Enablement Plan
- DEP SME - DEP Subject Matter Expert
- PIA - Privacy Impact Assessment
- SbD - Secure by Design
- SIA - Security Impact Assessment
- TC - TELUS Communications
- TI - TELUS International
- TH - TELUS Health

Document Control

Version	Date	Issued By	Approved by	Summary of Changes
1.0	January 23, 2023	Juan Arango, Purple Kumai	Rohin Bansal	Version 1.0 finalized for Director-level approval