EU *General Data Protection Regulation* FAQ

An Introduction to how GDPR impacts the Envestnet | Yodlee Platform and Services

January 2018

GDPR Impact and Posture

Is Yodlee GDPR Compliant?

Yodlee's Services and the Yodlee Platform will comply, as your data processor, with the EU General Data Protection Regulation (GDPR) on or before 25 May 2018. Yodlee will have the required technical and organizational safeguards to ensure that the personal data of your customers are protected and that, through you, their rights over their data are satisfied.

How does Yodlee fit into the current regulatory requirements?

Yodlee has operated in Europe since 2002 as a data processor under the EU Data Protection Act (DPA). Yodlee's privacy data handling program has consistently received independent validation by TrustARC (formerly TRUSTe) for US-EU Safe Harbour, US-Swiss Safe Harbour and now EU and Swiss Privacy Shield. Yodlee has, and will continue to execute EU Standard Contract Clauses with clients who desire that additional level of assurance. The Yodlee Platform and the processes that we use to develop, deliver and support our services have mature safeguards and governance overseen by an independent security, privacy, risk and compliance function, as well as receives regular certification by independent assessors and clients.

What is Yodlee's current GDPR compliance posture?

As a responsible member of the global financial ecosystem, Yodlee tracks all emerging global regulations, standards and practices to ensure adherence to applicable requirements. We have been very active with PSD2 and GDPR to ensure that we continue to be a reliable service provider to our EU clients. Specifically:

- ✓ Yodlee's internal compliance, security, privacy and legal teams have engaged with outside experts to conduct updated privacy impact assessments of Yodlee's services, to conduct a data protection impact assessment and to determine how each requirement of GDPR applies to our services.
- ✓ We have engaged an expert EU-based firm to guide us in the role of Data Protection Officer (DPO) and fulfill those responsibilities in a DPO-as-a-Service capacity.
- ✓ We have engaged expert outside counsel to provide us with legal opinions on how GDPR impacts our aggregation and analyses services, as well as any contract modifications that may be required to existing and new client engagements.

Protecting Your Customers

As your data processor, we support you by powering your solutions and protecting your customers. Here's some things we think you'd like to know.

Communications

You need to tell your customers what data you're collecting, with whom you are sharing it, where it's stored and for how long. Using Yodlee's APIs, you can manage this data collection and storage though-out the customer journey. We also provide you transparent access to the information you need to communicate with your customers about Yodlee's processing role.

Consent

Yodlee's Services are 100% customer permissioned. We provide you with clear guidelines for crafting consent flows to comly with GDPR and PSD2.

Access & Portability

It's your customers' data. Using our APIs, you can allow them to access and download their data when they want it.

Warnings and Breach Notifications

Our contract with you requires that we notify you of a data breach or any unauthorized access to your customers' data. We have robust security incident detection and management programs that meet rigorous financial industry standards.

Marketing

We do not market to your customers. In fact, we are prohibited from doing so per our contract with you.

Profiling

If you are using Yodlee's Services for processing applications for loans or making other decisions, we have additional safeguards and governance controls to support these compliance requirements. It's imporant to let us know this when you sign-up so we can guide you appropriately.

Safeguards

Yodlee maintains bank-grade security safeguards for our entire Platform to provide your customers' data from external and internal threats. Please see *Yodlee's Security FAQ* for more information about these programs.

Data Transfer

Clients who deploy in Yodlee's US data centres, may rely on our Privacy Shield compliance status or may request Controller-to-Processor Standard Contract Clauses.

Right to be Forgotten

Customers' information may be updated or deleted using Yodlee's APIs from within your application or as separate administrative functions. As the data controller, your customers' personal data is fully under your control.

Data Classification and Scope

What data is in scope for GDPR

The Yodlee data model is organized by a set of layered data classification schemes. From a GDPR perspective, there are three data classifications in scope:

Customer Data: Information provided by the client as part of user registration and the information gathered from external sites at the request of the user. Customer Data *may* contain Personal Data of our clients' EU customers, and is therefore in scope for GDPR.

Usage Data: Data about the client's use of the Yodlee Platform. Usage Data *does not* contain Personal Data of our clients' EU customers, and is not in scope for GDPR.

Aggregated Data: De-identified (i.e. pseudo-anonymised) account and transaction data from across the Yodlee Network. Aggregated Data is in scope for certain requirements of GDPR, notably consent from the data subject for this secondary processing.

How is Customer Data in scope for GDPR?

Customer Data is defined as the data our clients provide to register their customers on the Yodlee Platform, as well as the data we retrieve on their behalf, and with the customer's explicit permission, about the customer's financial accounts. Customers are registered on the Platform by the data controller (i.e. the Yodlee client) using generic indirect identifiers (GUIDs) that are not Personal Data. As customers link their external accounts, they entrust their access credentials (e.g. passwords or tokens) for each institution. These credentials are Personal Data as they identify the account holder. The data

Yodlee retrieves on their behalf may contain direct identifiers that are Personal Data (e.g. account holder name, full name or email address in a credit card transaction description). Accordingly, Yodlee has enacted safeguards and governance over the transmission, storage and processing of Customer Data to comply with the current DPA and the GDPR.

Why is Usage Data not in scope for GDPR?

Usage Data is information about our clients' use of the Yodlee Platform, such as API calls, performance metrics and other technical details. As such, there is no Customer Data and therefore no Personal Data contained in Usage Data. Furthermore, the usage is of the data controller, not the data subject.

What is Aggregated Data and how might it be in scope for GDPR?

Aggregated Data is derived from Customer Data from across the Yodlee network. As part of the derivation process, Yodlee removes attribution to the source (i.e. controller) and the customer (i.e. subject) as part of a comprehensive de-identification process, as well as direct identifiers (i.e. Personal Data) and known indirect identifiers (e.g. transaction IDs). The resultant end product meets the standard of "protected de-identified" which requires that the data has all direct and all known indirect identifiers removed or transformed and there are technical, organization and administrative controls over the handling of the data to prevent re-identification of the users. In DPA/GDPR terms, the data is pseudo-anonymized. We adhere to this standard rather than full anonymization to strike the right balance between consumer protection (i.e. negligible risk of re-identification) and usefulness of the data (i.e. ability to remove bias in the data set for accuracy in analytics.)

How does Yodlee use Aggregated Data?

Yodlee uses Aggregated Data for analytical research of consumer spending, saving, borrowing and investment behaviors at the aggregate level. We also perform behavior and trend analysis for clients, as well as license Aggregated Data panels to clients so they can conduct their own behavior and trend research. This processing and use is under the oversight of our compliance, risk, privacy and security programs, including independent 3rd party assessments.

Data Location and Access

Where does Yodlee store the data of its EU clients?

Yodlee operates from data centres around the globe, including the US, Canada, Australia, India and the UK. Clients are deployed in the data centre in their region or, at their request, in the US data centres.

Is there cross-border data transfer of client data?

No, the Yodlee Platform is designed with localization controls so that cross-border data transfer is neither required nor allowed without instructions from our client. To deliver and support the services, Yodlee does conduct cross-border data access under technically enforced role-based access controls that enforce the prohibition of transfer of Personal Data. These controls are described in more detail in the *Yodlee Security FAQ*.

What's Next?

In early 2018, Yodlee will complete the engagements with outside experts to finalize our compliance posture so that we may update our safeguards, governance, contracts and processes. We will provide an update to our

clients and prospects no later than 1 April 2018 to ensure full readiness by 25 May 2018 when GDPR enforcement begins.