Data Privacy and Compliance - FAQ

We have created an FAQ below to support questions related to how the DigiFish Analytics Data Pool known as LinkLake™ is generated and how applicable consumer privacy and regulatory compliance are addressed.

How does DigiFish collect the data put into LinkLake?

DigiFish does not collect data directly from the consumer. DigiFish contracts with Contributors to utilise their consumer data assets. DigiFish manages deep profiles around people, places and businesses geo-tied to their digital footprint. From this we build a comprehensive identity graph with interconnected entities across multiple contact pathways both online and offline.

What DigiFish Requires from its Contributors?

DigiFish contracts with Contributors such that they warrant:

- The Consumer records are collected in compliance with the Australian Privacy Act 1988.
- The Consumer consented / opted-in such that their details can be utilised to fulfil DigiFish Use Cases.
- The Consumer consented / opted-in such that their details can be provided to third party organisations downstream.
- The Consumer consented / opted-in such that their details can be provided to Third Party Organisations outside Australia.
- The Contributors have a robust and effective Consumer opt-out process from the Consumer and to and from DigiFish.
- The Consumer has been informed of the Contributors opt-out process.
- The Contributors have a data breach policy.
- The Contributors consent to the DigiFish Privacy compliance attestation audit.

Does DigiFish Consider the Consumer?

DigiFish as part of its core ISO 27001 Information Security Management System implementation considers the Consumer as an 'Interested Party'. As such they have legal and consideration rights in the handling, storage, use and disclosure of their information by DigiFish. We therefore have designed our Information Security Compliance and Privacy Compliance program to protect the Consumer as an Interested Party.

Understanding our Contributors.

Our Contributors are sourced from three types of industry leading data generating organisations, these include online mobile device driven location data, offline opt-in lead generation data and offline attribute data at address and person level.

In reference to our Contributors when we refer to DigiFish collection practices below we are referring to our Contributors collectively.

DigiFish captures data at a broad level for both Consumers and Mobile Location Data and addresses applicable privacy and compliance. Note that while apps and sites, the same privacy compliance applies to all data collected and managed by DigiFish.

All data collected, and associated partners are required to, support clear and compliant privacy notices and opt-in/out management that allow for collection, use, and distribution to 3rd parties. Noncompliant data that is identified is suppressed as detailed below and will not be delivered to customers.

What rights and permissions do you have to the data that you make available to your customers?
DigiFish maintains complete rights to license the data collected to customers for any legally permissible purpose including but not limited to marketing, advertising, publishing, lead generation, analytics, fraud prevention, credit scoring, debt collection, and contextual recommendations.

We set a minimum Use Case standard for all ingested data such that it may be utilised for analytics, segmentation, indirect marketing and summary modelling.

How do we provide you data?
DigiFish provides its data to clients either:

- Licenced Platform – client can upload their PII data and link to the DigiFish LinkLake
- Data Load – client can receive a bucket of selected LinkLake data.

How can DigiFish Audience Intelligence be transferred to a non-PII environment/application?
DigiFish's deep audience segments on consumers can be attached to device ids, cookies, hashed emails. In a non-PII supported environment, deep consumer intelligence will go out as segments without attachment to core identifying information. For example, in a programmatic environment when requests come in against a hashed email, a device id , cookie, or an ip address, DigiFish matches the input against its base and returns segments such as pet-owner, >120k income, outdoor enthusiast, executive at a FT500 company, age 35-45, male, visited x, y z, places and searched for keywords/concepts/tech domain related web searches in last couple of weeks. This external intelligence would help contextualize offer/recommendation and personalization. So in essence, all PIIs can be fully abstracted in the resulting feed/dataset/platform output. Customers can receive machine-readable intelligence tied to some ids, cross-device ids or hashed ids.

If a brand wants to extend intelligence on its consumer base, DigiFish can accept input with non-PII data (a set of hashed emails, device ids, cookies, ip addresses or other) and append deep intelligence against the input. For PII level enhancement, DigiFish dataset, platform, tools or a subset of it could be taken in-house for append and aggregation.

Do you follow any self-regulatory practices?
DigiFish follows closely and adheres to the generally accepted principles of many organizations including ISO 27001, NAI, DAA, and others.

What options do you provide, if any, for consumers to opt-out of your data practices?
DigiFish only works with data that is collected with clearly stated opt-in and easily accessible opt-out for consumers.

How do you avoid collecting data from child-directed websites, apps or other sources, owned and pirated or via partner relationships?
No data is collected or maintained for people under the age of 18 years.

How are you addressing compliance with the California Consumer Privacy Act (CCPA)?
DigiFish has been diligently working with its Contributors actively to ensure compliance with CCPA such that only data that is CCPA compliant is collected and passed along to customers.

- **Updated Privacy Policies** - Using plain language, avoiding technical or legal jargon, describe ALL PII collected, the purposes for which PII will be used.
- **Includes** a section for California residents that among other things:
    - enables users to request what PII the company has collected about a user, the categories of PII sold or disclosed, and sources of PII
    - enables users to request the deletion of PII about them
    - informs users about their right to opt-out of the sale of their PI
    - Includes at least two methods (e.g. web form, email) for users to exercise their rights.
- **Do Not Sell Link -** CCPA requires a clear and conspicuous "Do Not Sell My Personal Information"
- **Opt-In Notice and Consent, and "Signed Attestation"** - Based on CCPA and NAI standards, before is collected, a notice to users must inform them that their data will be collected and shared with partners, including use case categories. DigiFish has actively worked with partners to implement and will make available to customers representative samples of notice for customers to keep on file and will update as needed.
- **Audit Flag Columns Included in Daily Data Feed** – DigiFish will make available to customers the ability to include the following flags in the data delivered:
    - "ccpa_dns_present" will equal 1 for all rows if a CCPA compliant Do Not Sell opt-out links were in place at the time the data was collected, and the user has not opted out.
    - "consent_obtained" will equal 1 for all rows if the user properly opted-in with CCPA compliant notice and consent.
- **Updated "Consumer Requests" File** - For consumer opt-out requests, DigiFish will make available to customers a CSV file of affected records (i.e. device id's). This file would be titled YYYY/MM/DD/consumer_requests/Pub_id (if applicable). The columns of this file should be "applicablerecord_id," "action" (which would be "opt-out"), and UTC timestamp.

How does GDPR impact your company's data collection or aggregation policies in the EU and how you are addressing?
DigiFish has been actively working with our partners to ensure opt-in/opt-out and terms of use are updated, clear, and comply. The result is that our supply of data in the EU has the following two fields to EU data:

• **GDPR**: mark 0 or 1 (1 is restricted uid and 0 is non-restricted uid) [if a user is located in the EU then this field must be set to 1]
• **GDPR_consent**: This is the IAB consent string which is a daisy bit encoded in base64. Always have this column present even if gdpr=0, just keep the consent blank.