250ok GDPR Handbook

Introduction

The 250ok GDPR Handbook exists to clearly explain the processes by which 250ok collects and stores sensitive or permission-based data. Since we're primarily a data processor, it's important to distinguish our responsibilities versus those of our customers, as we ensure compliance with the General Data Protection Regulation (GDPR).

If there are questions about any part of this handbook, please do not hesitate to contact our legal department: legal@250ok.com.

250ok's Role in the Data Collection Process

It's important to understand the distinction between *data processor* and *data controller*. Here is the distinction, as related to GDPR Article 4 "Definitions" items 7 and 8:

If your organisation is determining the purpose of the storage or processing of personal information, it is considered a controller. If your organisation stores or processes personal data on behalf of another organisation, it is considered a processor.

250ok is primarily a *data processor*, because we process and store the majority of our data from and for someone else. Here is a detailed list of personal data we store as a *data processor*:

- **Feedback loop complaints** forwarded to 250ok from internet service providers and/or mailbox providers, or forwarded from 250ok customers. Feedback loop reports are provided in two formats:
    - Direct parsing of complaints via 250ok's SMTP servers
    - Complaints submitted from email service providers via webhook
- **Webhook-based analytics events** including email addresses, geolocation, opens, clicks, bounces, and deferrals, forwarded to 250ok from email service providers or 250ok customers.
- **Pixel-based analytics events** including email addresses, geolocation, user agents, opens, and mailbox providers. Pixel-based events originate from customers embedding the 250ok tracking pixel into their email messages.
- **DMARC reports** originate from internet service providers and mailbox providers, and are forwarded to 250ok on behalf of the customer. While aggregate DMARC reports do not contain any PII, it's possible for forensic DMARC reports to contain an email address if the customer configured their policy to send us such reports.

Though we operate as a data controller in a limited capacity, this list provides insight into the personal data we store as a *data controller:*

- **Website contact forms** including the full name, email address, IP address, phone number, employer, and job title of those contacting 250ok for sales, support, or general inquiries.

- **Off-site leads** including the full name, email address, phone number, employer, and job title of potential customers originating from marketing campaigns, industry events, or referrals from partners.
- **User accounts** for accessing the 250ok platform. Information included contains full name, email address, job title, phone number, and employer. This may also include the same data on child account users that access our platform via the contracted entity.

Transmission of Data, Data Storage, and Data Retention

In 250ok's role as a *data processor*, we collect and store data from our customers (*data controller)*. It is the sole responsibility of 250ok's customers and clients to receive direct consent (opt-in) from their users before transmission to 250ok. Under no circumstance does 250ok share the data of its customers with third parties. Outlined below is a full reference of the types of data processed and stored by 250ok on behalf of its customers:

GDPR Data Map

Source How was this data collected?	**Personal Data** What personal data is being collected?	**Reason** Why are you collecting this data? Marketing, CRM, analytics or other?	**Handling** Explain how you will store the data, how it will be processed and who has access to it.	**Disposal** When is this data disposed?
Analytics events (via pixels our customers embed in emails)	Email address, mailbox provider, IP address, geolocation, user agent	This data enables us to measure the performance of an email campaign based on demographic factors.	See Reference: Data Collection & Storage	2 years
Analytics events (via SMTP-based webhook events forwarded from our customers)	To address, mailbox email address, provider, IP address, geolocation, user agent	This data enables us to measure the performance of an email campaign based	See Reference: Data Collection & Storage	2 years

		on demographic factors.		
Feedback Loop (FBL) complaints , forwarded from customers (via webhook or ARF)	Email address	FBL complaints allow us to aggregate complaints by email address to suggest suppression	See Reference: Data Collection & Storage	2 years
DMARC reports (via SMTP messages)	Email address (occasionally occurs in forensic reports)	DMARC report processing is required for determining if fraudulent activities are taking place on a DMARC-protected domain	See Exhibit A: Data Collection & Storage	2 years

As *data controllers*, the reference table below outlines the types of data processed and stored by 250ok on behalf of itself:

GDPR Data Map

Source How was this data collected?	**Personal Data** What personal data is being collected?	**Reason** Why are you collecting this data? Marketing, CRM, analytics or other?	**Handling** Explain how you will store the data, how it will be processed and who has access to it.	**Disposal** When is this data disposed?
Website contact and demo forms (submitted via WordPress by individual prospects)	Full name, email address, IP address, phone number, employer, job title	These forms are responsible for receiving new business inquiries and coordinating follow-up	Forms are submitted on the WordPress site and stored locally on a MySQL database, as well as Salesforce CRM	Indefinite

User accounts for 250ok platform	Full name, email address, phone number, employer, job title	This data is utilized to manage access to the 250ok platform.	Data is stored in SQL database and presented inside the 250ok application.	Determined by length of contract.

Right of Access

In accordance with Article 15 of the GDPR, 250ok will aim to provide its customers with transparency and ease-of-access to their data. We'll provide the forms and tools necessary for our customers to access, export (or transfer), erase, or anonymize data subjects by request, and 250ok will honor the request within 30 days. Customers can also review or correct the information associated with their account instantly, at any time.

In instances in which 250ok is the *data controller,* customers can review or correct the information associated with their account. Additionally, they'll have the same access to the forms and tools necessary to access, export (or transfer), erase, or anonymize their personal data. Lastly, customers can restrict the processing of data subjects at any time by pausing data forwarding to 250ok.

Privacy Policy

250ok has addressed Right of Access (Article 15) in its privacy policy (https://250ok.com/privacy/):

You may access, correct, request deletion or request a copy of any or all of your personal data in our possession by emailing us at support@250ok.com, and we will honor your request within thirty (30) days. If we incur expenses to comply with your request, we may charge you a reasonable fee to cover these expenses, if permitted by law. If you believe any of the personal data we have collected from you is inaccurate, you can email support@250ok.com with a request to update this information. We will honor your requests within a reasonable timeframe.

Management and Accountability

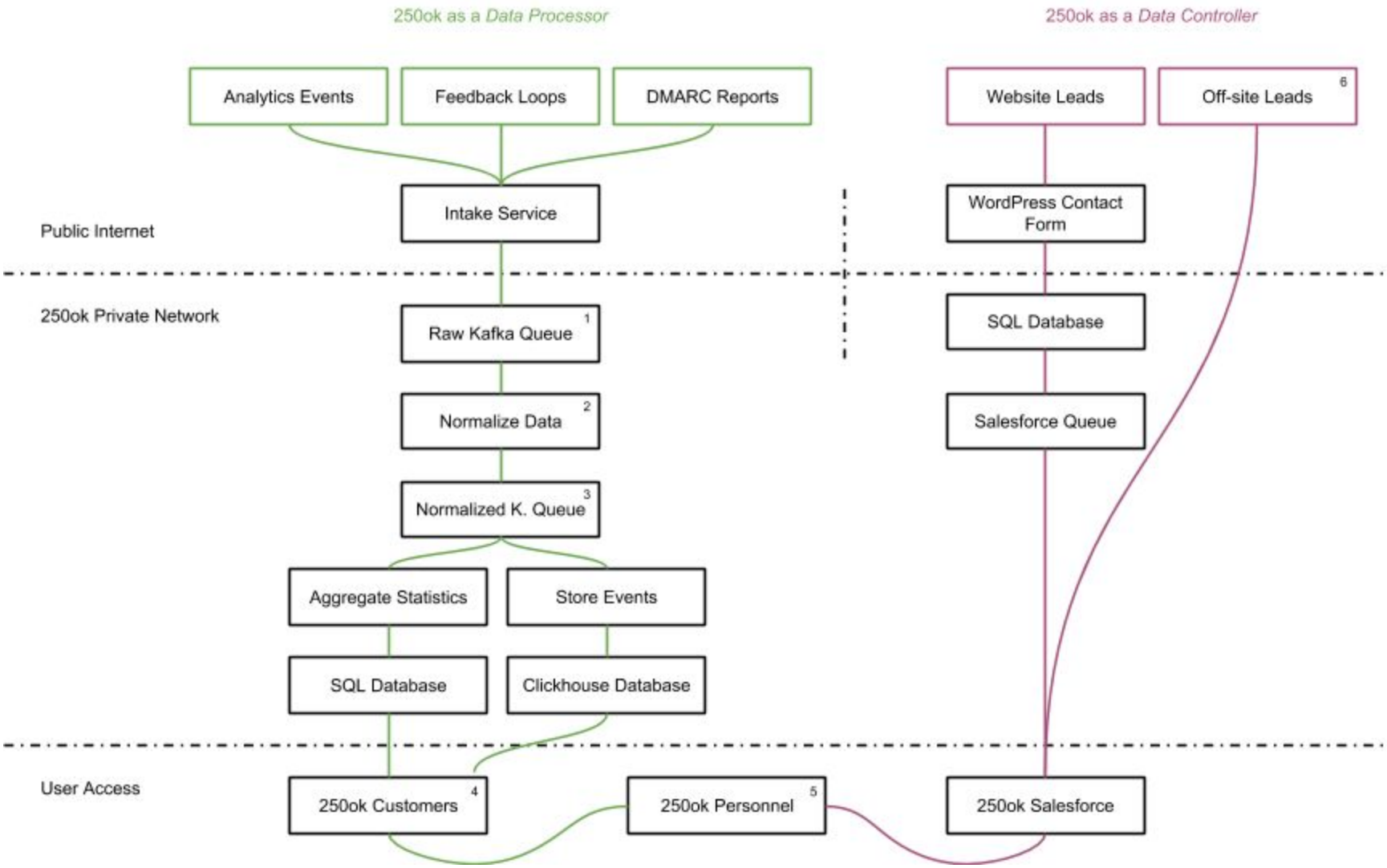
250ok's designated data protection officer (DPO) is Ryan Pfenninger, 250ok's chief technology officer. It is the responsibility of the DPO and other privacy-centric roles within 250ok (i.e. director of privacy) to ensure decision-makers are up-to-date about the importance of data protection legislation and best practices. It is the responsibility of the DPO to report data breaches to local authorities, including what data was lost, what the consequences are, and what countermeasures are being taken.

Additionally, all new 250ok employees are required to complete New Employee Cyber Security and Privacy Orientation, which covers potential risks and vulnerabilities, best practices, and how to properly safeguard and dispose of sensitive information.

Obligations of 250ok Customers

1. Consent: It is the sole responsibility of 250ok's customers and clients to receive direct consent (opt-in) from its users before transmission to 250ok. This includes consent to international data transfer until such time 250ok deploys a European data center.
2. Privacy policy meeting GDPR requirements: As outlined in Article 15 of GDPR, all *data controllers* (customers) utilizing 250ok as a downstream processor must address Right of Access in its privacy policy.
3. Right to Access for Data Controllers: 250ok will provide a "GDPR Form" by which customers can access, export (or transfer), erase, or anonymize data subjects by request. In the event access is requested for data 250ok does not own, the *data controllers* (customers) will be notified directly and they will become responsible for fulfilling the request.
4. Data Processor Agreement (DPA): All 250ok customers will be asked to sign and return a Data Processor Agreement.

Reference: Data Collection and Storage



Reference: Data Collection and Storage (Appendix)

1. All events route through the “intake” service, a receiver that takes in data in a number of formats. Depending on the format or type of data, it’s then routed to the appropriate Apache Kafka queue for additional processing and normalization. Data can be temporarily stored in these Kafka topics for two (2) to seven (7)days, depending on the type of data, which is necessary for redundancy and correcting inaccuracies.

2. Data is then pulled from the raw queue, normalized, and transferred to the normalized Kafka queue. The same retention necessities apply.

3. Once data is cleansed and normalized, it’s matched to a 250ok customer account and stored in the database. 250ok uses multiple database storage technologies, depending on what is most suitable for performance. Normalized events are stored in our Clickhouse database, whereas aggregate statistics are primarily stored in SQL databases.

4. Inside the 250ok application, customers can access the data associated with their account. No personal data is shared across customers or customer accounts.

5. Data is accessible by 250ok support and account management personnel. Support personnel have the ability to log into customer accounts to help them troubleshoot problems and resolve support issues. Similarly, account management personnel can log in to custom accounts to answer questions from the customer and assist them in training.

6. Although website contact and demo forms were documented in the GDPR Data Map, there are also instances in which 250ok handles personal data from off-site lead sources and stores data subjects in Salesforce. Such sources can include marketing campaigns, industry events, or referrals from partners.