fimble

# Data Privacy

**Last update:** March 25th 2025

# Table of contents

- Aim
- Storing & Processing of Data
- Data Protection Application
- Thank you

# Aim

- The aim of Fimble and Enray platform in general, is to store as little private data as possible across all contact types while at the same time retaining the information necessary for processing and delivering the transactions safely as well as building a robust customer profile that can be used in target marketing activities.

- At the same time, contacts who are willing to share more information with the business can do so through a variety of tools to produce effective profiling and behavioural statistics.

- The scope is not limited only to customers but also to employees, leads, vendors and resellers.

- Due to the various ways of interpreting the May 25th 2018 GDPR, Fimble provides the necessary tools to configure the privacy options according to your legal dept's requirements.

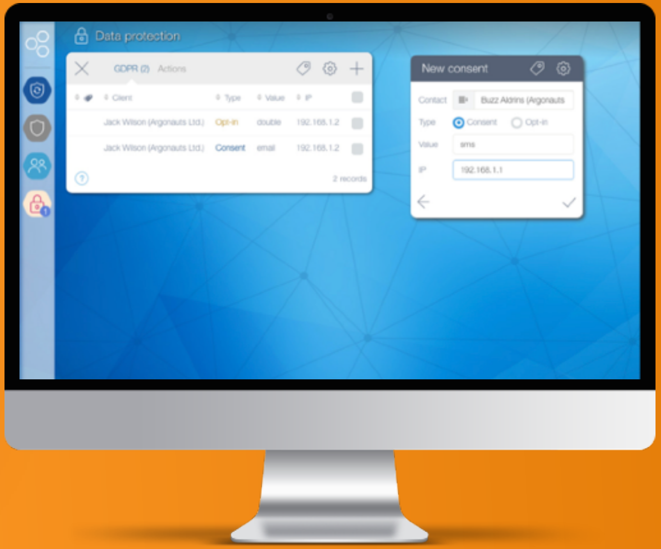
# Storing & Processing of data

- Sessions & cookies are properly destroyed after expiry
- All connections are performed through 2048-bit Grade A+ SSL
- Critically sensitive data such as passwords are always encrypted
- Credit card details are never stored in the system, even with card tokenization the data is fetched from the payment gateway and includes only the card type, the expiry date and the last 4 digits.
- Sensitive user activity is tracked only after consent
- Customers can only be communicated after their consent and they can change their preferences at any time
- Usage statistics such as Google Analytics and Hotter are collected anonymously
- All database information is protected with a Data at Rest Full-Disk Encryption
- Privacy policy, Terms & Conditions and Transaction Security are public and always accessible from every page
- Servers are continually patched and tested for vulnerabilities

# Data Protection

- In addition to the above, Fimble offers a new application that is included for free in all deployments of Fimble version 4.0 and newer, focusing on protecting your contacts data.

- This application is aimed to provide you with the tools necessary to perform private data manipulation tasks on time, according to the General Data Protection Regulation guidelines.



| | Client | Type | Value | IP |
|---|---|---|---|---|
| | Jack Wilson (Argonauts Ltd.) | Opt-in | double | 192.168.1.2 |
| | Jack Wilson (Argonauts Ltd.) | Consent | email | 192.168.1.2 |

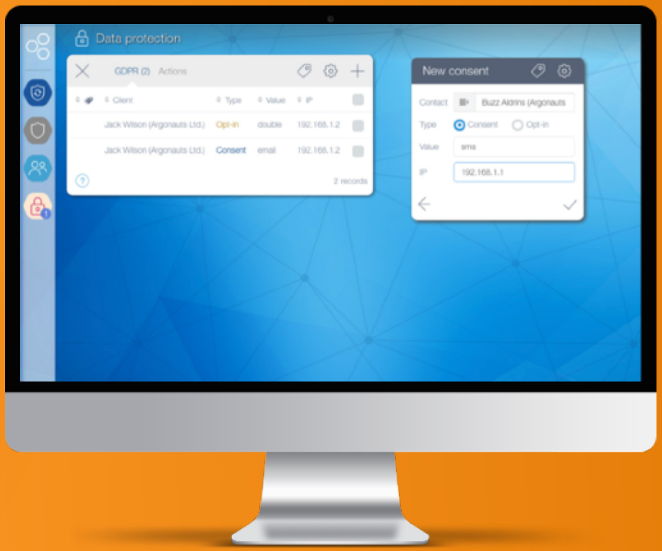
2 records

Contact: Buzz Aldrins (Argonauts
Type: ● Consent ○ Opt-in
Value: sms
IP: 192.168.1.1

# Data Protection

Data Protection application features include:

- List of all consent and double opt-in information for all of your contacts (internal users, clients, leads, vendors and resellers)
- Detailed log that shows all activity relating to the creation, deletion or modification of contact data
- Tool to automatically deliver or delete a contact's private data from the whole database
- Ability to request the deletion of the automatic cloud backup
- Settings to define what type of consents you require from your contacts
- Aggregated information on the consent and opt-in confirmations your business has received



Data protection

GDPR (2) Actions

| Client | Type | Value | IP |
|---|---|---|---|
| Jack Wilson (Argonauts Ltd.) | Opt-in | double | 192.168.1.2 |
| Jack Wilson (Argonauts Ltd.) | Consent | email | 192.168.1.2 |

2 records

New consent

Contact: Buzz Aldrins (Argonauts

Type: ● Consent ○ Opt-in

Value: sms

IP: 192.168.1.1

# Data Points

The following data points are collected by the system by default and some may be deactivated.

- First Name
- Last Name
- Email
- Cellphone number
- Full address
- Address coordinates
- Encrypted password (cannot be decrypted, it is only used for authenticating to make sure it is matching the one typed, which is also encrypted)
- GDPR consents (these are dynamic based on market's legal requirements or translation/enforcement of the privacy policy/GDPR guidelines)
- Card type & last 4 digits
- Order history with everything related to the transactions (items, preferred channels, preferred day/time, average ticket, preferred payment method, etc.) based on which some additional KPIs are generated (for example retention, frequency index etc.)
- Coupons (reserved/assigned & used)
- Offers used (e.g. 1+1 Wednesday Happy Hour)
- Tips
- Rewards points, accumulation & redemption history
- Order taking time
- Complaints
- Favorite items
- Favorite orders
- Customized products
- Buying habits
- Customer segmentation based on activity (usually purchasing activity e.g. number of orders, revenue etc.)
- Communication (history & content) such as emails, SMS & push notifications
- Read status on emails
- Customer tags (these are dynamically set by the administrator and not collected but rather assigned internally, for example "VIP customer")
- Logins*
- User agent meta data* (Browser/Device, OS, resolution, IP, Geolocation, network speed)
- Session* (for remembering the account)
- Cookies* (mostly website preferences e.g. Language, abandon basket contents etc., applicable only for web apps)
- LocalStorage* (Mostly app preferences e.g. Dark theme, remember account, applicable only for mobile apps)

# Data Points

- When the customer selects guest checkout to place an order without creating an account, then the majority of the previous Data Points is not collected. The PII data that is needed to facilitate the actual order e.g. address for delivery is kept for 30 days and then deleted automatically and then everything that remains is simply on the actual transaction which is for a generic "Retail customer" based on the commercial/IRS requirements on keeping transactional records that supersede the GDPR regulations.

- Additional data can be collected (e.g. date of birth, gender etc.) if the business elects to optionally use some of the marketing tools that allow them to do so, for example customer satisfaction surveys, online contests etc. These data points are dynamic which means they can be set by the business dynamically and Fimble has no control over this.

- For orders via POS, Drive Thru, Kiosk Ordering, QR Pickup Ordering & QR Dine In Ordering, since the majority of the transactions are unauthenticated (or guest checkout by default) there is no PII data collection except if the customer authenticates by either scanning/typing their rewards card or a non-recurring coupon that was assigned to his/her account (e.g. sorry coupon after filing a complaint). In this case the majority of the above are collected (if switched on) except the last 5 (marked with an asterisk) which are not applicable.

- In practice and according to Fimble's terms of use and the agreements in place, the data is 100% owned by the business.

# Thank you!

We would like to thank you for your time.

For more information you can visit www.enray.io/privacy or send us your email at privacy@enray.io