

Privacy - Third Party Apps and Services – v1.0 – Published 01.03.2021

In order to provide some of the functionality on the Wonderful Payments Website and associated services, we have to share information and personal data with some third party processors and their respective applications.

Listed here are those processors, a brief description of what data is transmitted to them and how we've vetted them and what agreements are in place.

A number of our service providers who have a presence in the US, have participated in the EU-US Privacy Shield Framework and have certified with this programme, as identified and explained further below. Although the Court of Justice of the European Union issued a judgment in July 2020 declaring as invalid European Commission Decision 2016/1250 (on the adequacy of the protection provided by the EU-US Privacy Shield), this decision does not relieve participants in the EU-US Privacy Shield of their obligations under the framework. As stated in our privacy notice, appropriate and adequate safeguards have been provided in relation to such transfers to such transfers, including for example, adoption of Standard Contractual Clauses approved by the European Commission in our contract with the party importing the personal data.

Amazon

We use Amazon Web Services (AWS) to host the Wonderful Payments Website Platform, therefore all user and charity data is stored on servers in Amazon's Data Centre's. Our main point-of- presence (POP) is that of their UK (London) DC, however at times where there may be increased traffic or maintenance on Amazon's infrastructure, this data may be transferred and made available to other Data Centre's within their network for resiliency purposes. Amazon participates in the EU-US Privacy Shield Framework and has certified with this programme. Our relationship with them is governed by their Terms of Service, and a Privacy Policy and Data Processing Addendum in line with GDPR Requirements. You can read more about Amazon's AWS Privacy Policies here: <https://aws.amazon.com/privacy/>

Apple

We predominantly use Apple hardware and their software solutions, including iCloud. Wonderful Payments Staff utilise the secure notes applications for making notes that may temporarily contain personal information during the course of an enquiry, complaint or other such issue that requires a resolution, and subsequently a response.

Our internal documents and notes pertaining to interactions with customers (containing email addresses, phone numbers and users' names) are written in their suite of Collaboration tools, which uses automatic saving and backup to their cloud storage service, iCloud.

Apple participates in the EU-US Privacy Shield Framework and has certified with this programme. Our relationship with them is governed by their Terms of Service and Apple uses approved Model Contractual Clauses for the international transfer of personal information collected in the European Economic Area. More information can be found <https://www.apple.com/uk/legal/privacy>

Intercom

We use Intercom for our support desk. Charities will have their email address and contact name, plus the body of their email, stored on Intercom's servers in order for us to address any support queries. Internal, secure communications between staff may also have this data transmitted when an issue is investigated or escalated.

Our relationship with them is governed by their Terms of Service, and a Privacy Policy and Data Processing Addendum in line with Data Processing Requirements. You can read more about their data processing and privacy commitments here:

<https://www.intercom.com/legal/privacy>

Cloudflare

We use Cloudflare for DNS Services, Security and their Content Distribution Network, allowing us to manage traffic more effectively to the Wonderful Payments site and secure it from digital attacks and malicious activity. Cloudflare has access to the URL navigated to and what IP Address has accessed it. All data that is transmitted via the web to and from the Wonderful Payments Platform traverses Cloudflare's systems, however Cloudflare does not have access to this data.

Cloudflare participates in the EU-US Privacy Shield Framework and has certified with this Programme. Our relationship with them is governed by their Terms of Service at

<https://www.cloudflare.com/terms/>, and a Data

Processing Agreement here <https://www.cloudflare.com/privacypolicy/>

DigitalOcean

We use DigitalOcean for hosting some of our sundry services that are not hosted on our central infrastructure with AWS. A replica of charity and user data is stored on DigitalOcean servers located in London for disaster recovery and backup purposes. Some of our redirection services are also operated here, such as for old links to charity pages.

DigitalOcean participates in the EU-US Privacy Shield Framework and has certified with this programme. Our relationship with them is governed by their Terms of Service at

<https://www.digitalocean.com/legal/terms-of-service-agreement/>, and Data Processing agreement at <https://www.digitalocean.com/legal/data-processing-agreement/>.

Dropbox

We use Dropbox for storing company documents and encrypted backups of platform data, which includes charity data.

Dropbox participates in the EU-US Privacy Shield Framework and has certified with this programme. Our relationship with them is governed by their terms here:

<https://www.dropbox.com/terms2018> and Data

Processing Agreement here <https://assets.dropbox.com/documents/en/legal/data-processing-agreement-dfb-013118.pdf>

.

Google Inc.

We use G-Suite for our internal and staff email communications, along with their calendar and contacts systems. Therefore Google may store our users' email addresses and names. We also use Google Analytics to collect anonymized statistical data about how users interact with our website and services.

Google participates in the EU-US Privacy Shield Framework. You can read more about Google's Policies here: <https://policies.google.com/>

WHYPAY?

We use WHYPAY?'s conference calling platforms, therefore whenever we engage with charities, suppliers or staff via their conferencing services, email addresses may be transferred to WHYPAY? for the purpose of managing meeting invitations and scheduling. WHYPAY? is a UK company and their terms and conditions can be found <https://whypay.net/tscs/> and are compliant data protection here: <https://whypay.net/privacy-policy/>

Mailchimp

We use MailChimp for sending opt-in marketing emails to charities who have signed up for our newsletters and marketing emails. User emails and names are transmitted and stored on MailChimp's servers. MailChimp has significant controls where communication options are concerned and users wishing to modify their preferences can do so from within the email they receive.

MailChimp participated in the EU-US Privacy Shield Framework and certified with this programme. Our relationship with them is governed by their current Terms here: <https://mailchimp.com/legal/terms/>, and Data Processing here: <https://mailchimp.com/gdpr/>

Nexbridge Communications

We use Nexbridge Communications for the majority of our telephone services and route our calls via their exchanges and platform. Any time we receive or make a call, Calling Line Identifier information will be stored on Nexbridge's Billing servers to allow them to bill us for the calls we make and receive. As a telecoms carrier, this data is also stored for communication legislation and regulatory investigation compliance purposes. While this data alone cannot be used to personally identify an individual, it is still in the scope of this document as it is information that is transmitted to a third party nonetheless.

Nexbridge is a UK company and our relationship with them and the processing of personal data is governed by their Privacy Policy <https://nexbridge.co.uk/privacy/>

Citizen

All payments processed on the Wonderful Payments platform are handled by open banking supplier Citizen UK Holding Limited, therefore bank account data, address data, email addresses and names will be transmitted to, and stored, by them in accordance with PCI DSS 3.2.

Our relationship with Citizen in the UK is through a contractual terms here: <https://citizen.is/terms-of-service> and their privacy policy can be found here: <https://citizen.is/privacy-policy>. Citizen is FCA authorised.

Slack

Slack is a secure encrypted internal staff collaboration tool used by staff for internal messaging, calling, conferencing and document sharing.

Slack participated in the US Privacy Shield and their terms and conditions can be found <https://slack.com/intl/en-gb/terms-of-service> and privacy policy here: <https://slack.com/intl/en-gb/privacy-policy>

Tresorit

We use Tresorit for secure transfer of sensitive documents as part of our Charity onboarding procedure. It is an end-to-end encrypted file sync and sharing service.

Tresorit is compliant with current data protection here <https://tresorit.com/gdpr> and further information of their Terms and Conditions can be found <https://tresorit.com/terms-of-use>.