

# One2Call Privacy Statement.

---

*Version: 1.0*

*Issue Date: 03/05/2018*

*Author: Alex Hodgson*

---

This privacy statement explains what personal data One2Call collects from you, through our interactions with you and through our products, and how we use that data.

## Personal Data That We Collect

It is One2Call's policy to limit as far as possible the amount of personal data it collects from its customers.

However, the data we collect can include the following:

### Name and contact data.

We may need to collect your first and last name, contact phone numbers and email address. We will only collect your own personal email and phone numbers where no business contact details are available, or your personal contact data is the main contact information for the business.

### Credentials.

We do not collect and store personal passwords, such as to your PC or laptop.

### Demographic data.

We do not collect data about you such as your age, gender, country and preferred language.

### Payment data.

We collect data necessary to process business payments, such as your banks account number (for BACS transfer) or bank card details (such as a credit card number), and the security code associated with your payment instrument. In most cases this should be business payment data, not personal payment data, unless your personal payment details are also the main payment accounts for your business.

### Device and Usage data.

We may collect data about your device and how you and your device interact with some of our products. For example, we collect:

- **Device, connectivity and configuration data.**  
We may collect data about your device and the network you use in order to fulfil our support commitments to your business. This may include data about the operating systems and other software installed on your device, and may including product keys. It may also include IP address, device identifiers (such as the IMEI number for phones), and regional and language settings.
- **Error reports and performance data.**  
We may collect data about the performance of the products and any problems you experience with them in order to fulfil our support commitments to your business. This data helps us to diagnose problems in the products you use, and to improve our products and provide solutions.

Product-specific sections below describe data collection practices applicable to use of those products.

## How We Use Personal Data

One2Call uses the data we collect for two basic purposes only:

- 1) to operate our business and,
- 2) to send communications, including promotional communications

## Operating our business.

We use data to provide, support and improve the products and services we offer and perform essential business operations. Examples of such uses include the following:

- **Providing the Products.**  
We use data to carry out your transactions with us and to provide our products to you. Depending on the product this may include passing your data on to a third party.
- **Customer support.**  
We use data to diagnose product problems, repair customers' devices and provide other customer care and support services.
- **Product activation.**  
We use data – such as device and application type, location and unique device, application, network and subscription identifiers – to activate software and devices that require activation.

## Communications.

We use data we collect to communicate with you and personalise our communications with you.

For example, we may contact you by phone or email or other means to inform you when new product features or services are available, to discuss contracts and licensing, update you or enquire about a service or repair request, invite you to participate in a survey, or inform you when you need to take action to keep your services running.

Additionally, you can choose whether to receive further personalised information via email subscription from One2Call on subjects such as special offers, business efficiency, new technologies, local interest, quizzes and events.

## Reasons We Share Personal Data

We share your personal data with your consent or as necessary to complete any transaction or provide any product or service you have requested or authorised.

We may share your details with our trusted service partners in order to set up services with them., such as you name, email address or phone numbers. For example, provisioning your Microsoft Office 365 account and mailbox will require at least your name and email address to be shared with Microsoft. See below for a full list of our trusted partners with whom your basic personal information might be shared.

When you provide payment data to make a purchase, we will share payment data with banks and other entities that process payment transactions or provide other financial services, and for fraud prevention and credit risk reduction.

We also share personal data with vendors or agents working on our behalf for the purposes described in this statement. For example, companies we've hired to support or assist in protecting and securing our systems and services may need access to personal data to provide those functions. In such cases, these companies

must abide by our data privacy and security requirements and are not allowed to use personal data they receive from us for any other purpose.

Finally, we will access, transfer, disclose and preserve personal data, when we have a good faith belief that doing so is necessary to:

- 1) comply with applicable law or respond to valid legal process, including from law enforcement or other government agencies;
- 2) protect our customers, for example to prevent spam or attempts to defraud users of our products, or to help prevent the loss of life or serious injury of anyone;
- 3) operate and maintain the security of our products, including to prevent or stop an attack on our systems or networks; or
- 4) protect the rights or property of One2Call, including enforcing the terms governing the use of the services.

## Security of Personal Data

We use a variety of security technologies and procedures to help protect your personal data from unauthorized access, use or disclosure. For example, we store the personal data you provide on computer systems that have limited access and are in controlled facilities. When we transmit highly confidential data (such as a credit card number or password) over the Internet, we protect it through the use of encryption.

## Where We Store and Process Personal Data

We store personal data on our own secure internal servers, or with third parties who provide cloud-hosted services to us and whose security standards we deem to be as secure or more secure than our own.

For details of the third parties we utilise and their own security and privacy policies please see our accompanying document **One2Call Cloud Service Provider Security Details**.

## Our Retention of Personal Data

One2Call retains personal data for as long as necessary to provide the products and fulfill the transactions you have requested, or for other essential purposes such as complying with our legal obligations, resolving disputes and enforcing our agreements. Because these needs can vary for different data types in the context of different products, actual retention periods can vary significantly.

The criteria used to determine the retention periods include:

- **How long is the personal data needed to provide the products and operate our business?**  
This includes such things as maintaining and improving the performance of those products, keeping our systems secure and maintaining appropriate business and financial records. This is the general rule that establishes the baseline for most data retention periods.
- **Is the personal data of a sensitive type?**  
If so, a shortened retention time would generally be appropriate.
- **Has the user provided consent for a longer retention period?**  
If so, we will retain data in accordance with your consent.
- **Is One2Call subject to a legal, contractual or similar obligation to retain the data?**  
Examples can include mandatory data retention laws in the applicable jurisdiction, government orders to preserve data relevant to an investigation or data that must be retained for the purposes of litigation.

## Third-Party Service Providers.

As noted above One2Call may need to share personal data with third parties who either provide services to us in order to run our business, or who provide services to us that we then resell to our customer base.

These providers can change over time as we change internal processes or sign up with new suppliers, but the third party providers who we will need to share personal data with in order to provide any of our services are as follows:

Provider name	Nature of service	Data shared	Security details
<b>Adobe Sign</b>	eSignatures	Name, email, phone number, mobile number, business address, bank details.	<a href="#">Adobe Trust</a>
<b>Xero</b>	Accountancy	Name, email, phone number, mobile number, business address, bank details.	<a href="#">Security at Xero</a>
<b>WorkflowMax</b>	Work Management	Name, email, phone number, mobile number, business details.	<a href="#">WFM Privacy Policy</a> (WFM owned by Xero)
<b>Hubspot</b>	CRM	Name, email, phone number, mobile number, business details, IP address.	<a href="#">Hubspot Data Privacy</a>
<b>Zendesk</b>	Support Portal	Name, email.	<a href="#">Zendesk Security</a>

## Changes to This Privacy Statement

We will update this privacy statement when necessary to reflect customer feedback and changes in our products. When we post changes to this statement, we will revise the version number and "last updated" date at the top of the statement. An archive of previous Privacy Statements will be available on request by email to [info@one2call.net](mailto:info@one2call.net).

## How to Contact Us

If you have a privacy concern or complaint please contact us by using any of the contact methods [on our website](#).