Data Protection and Privacy Policy

1. How your personal information is used.

In compliance with the new General Data Protection Policy Regulation (GDPR) we have updated our policies with regards to how we use your data below. This will be implemented from 25th May 2018. You don't have to do anything but if you have any questions, feel free to contact us on 0800 144 88 44.

Your information will be held by IFace Comms Ltd, a company registered in England with number, and whose registered office is at The Junction, Charles Street, Horbury, WF4 5FH. We are part of the iFace Group of companies and may from time to time share your information within the group.

2. How we use your personal information

This privacy notice is to let you know how companies within the Group promise to look after your personal information. This includes what you tell us about you, what we learn by having you as a customer, and the choices you give us about what marketing you want us to send you. This notice explains how we do this and tells you about your privacy rights and how the law protects you.

Our Privacy Promise

We promise:

- To keep your data safe and private.
- Not to sell your data.
- To give you ways to manage and review your marketing choices at any time.

This notice sets out most of your rights under the new laws.

3. Who we are

The iFace Group is made up of a group of separate legal entities. These include IFace Comms Ltd (Co no. 12097084) iFace Group Ltd (Co no. 1161821), Go Get Tech Ltd (Co no. 11219099) and iFace IT Ltd (Co no. 11947352). We will let you know which one you have a relationship with, when you take out a product or service with us.

You can find out more about us at www.ifacecomms.com

If you have any questions, or want more details about how we use your personal information, you can ask us by calling us on 0800 144 88 44 or emailing us at info@ifacegroup.com

4. How the law protects you

As well as our Privacy Promise, your privacy is protected by law. This section explains how that works.
Data Protection law says that we are allowed to use personal information only if we have a proper reason to do so. This includes sharing it outside iFace Group. The law says we must have one or more of these reasons:

- To fulfil a contract we have with you, or
- When it is our legal duty, or
- When it is in our legitimate interest, or
- When you consent to it.

A legitimate interest is when we have a business or commercial reason to use your information. But even then, it must not unfairly go against what is right and best for you. If we rely on our legitimate interest, we will tell you what that is.
Here is a list of all the ways that we may use your personal information, and which of the reasons we rely on to do so. This is also where we tell you what our legitimate interests are.

What we use your personal information for:	Our reasons	Our legitimate interests
• To manage our relationship with you or your business. • To develop new ways to meet our customers' needs and to grow our business. • To develop and carry out marketing activities. • To study how our customers use products and services from us and other organisations. • To provide advice or guidance about our products and services.	• Your consent. • Fulfilling contracts. • Our legitimate interests. • Our legal duty.	• Keeping our records up to date, working out which of our products and services may interest you and telling you about them. • Developing products and services, and what we charge for them. • Defining types of customers for new products or services. • Seeking your consent when we need it to contact you. • Being efficient about how we fulfil our legal duties.

What we use your personal information for:	Our reasons	Our legitimate interests
• To develop and manage our brands, products and services. • To test new products. • To manage how we work with other companies that provide services to us and our customers.	• Fulfilling contracts. • Our legitimate interests. • Our legal duty.	• Developing products and services, and what we charge for them. • Defining types of customers for new products or services. • Being efficient about how we fulfil our legal and contractual duties.
• To deliver of our products and services. • To make and manage customer payments. • To manage fees and charges due on customer accounts. • To collect and recover money that is owed to us. To manage and provide treasury and investment products and services.	• Fulfilling contracts. • Our legitimate interests. • Our legal duty.	• Being efficient about how we fulfil our legal and contractual duties. • Complying with regulations that apply to us.
• To detect, investigate, report, and seek to prevent financial crime. • To manage risk for us and our customers. • To obey laws and regulations that apply to us. • To respond to complaints and seek to resolve them.	• Fulfilling contracts. • Our legitimate interests. • Our legal duty.	• Developing and improving how we deal with financial crime, as well as doing our legal duties in this respect. • Complying with regulations that apply to us. • Being efficient about how we fulfil our legal and contractual duties.

What we use your personal information for:	Our reasons	Our legitimate interests
• To run our business in an efficient and proper way. This includes managing our financial position, business capability, planning, communications, corporate governance, and audit.	• Our legitimate interests. • Our legal duty.	• Complying with regulations that apply to us. • Being efficient about how we fulfil our legal and contractual duties.
• To exercise our rights set out in agreements or contracts.	• Fulfilling contracts.	

Groups of Personal Information

We use many different types of personal information, and group them together like this.

Types of personal information	Description
Financial	Your payment information including account details
Contact	Your business address and how to contact you.

Types of personal information	Description
Transactional	Details about payments to and from the accounts you have with us.
Contractual	Details about the products or services that we provide to you.
Locational	Data we get about where you are, such as may come from your service installation address or company registered address.
Behavioural	Details about how you use our products and services.
Technical	Details on the devices and technology you use with us.
Communications	What we learn about you from letters, emails, and conversations between us.
Usage Data	Other data about how you use our products and services.
Documentary Data	Details about you that are stored in documents in different formats, or copies of them. This could include things like your contracts with us and copies of email communication between us.

Types of personal information	Description
Consents	• Any permissions, consents, or preferences that you give us. This includes things like how you want us to contact you or whether you get paper invoices.

5. Where we collect personal information from

We may collect personal information about you or your business from other companies within the iFace Group and from these sources:

Data you give to us:

- When you purchase products and services with us
- When you talk to us on the phone or in person
- When you use our websites, mobile device apps, web chat services
- In emails and letters
- In customer surveys

Data we collect when you use our services. This includes the amount, frequency, type, location, origin and recipients:

- Profile and usage data. This includes the profile you create to identify yourself when you connect to our internet, mobile and telephone services. It also includes other data about how you use those services. We gather this data from devices you use to connect to those services, such as computers and mobile phones, using cookies and other internet tracking software.

Data from third parties we work with:

- Companies that introduce you to us.
- Fraud prevention agencies.
- Public information sources such as Companies House.
- Agents working on our behalf, such as channel partners.
- Government and law enforcement agencies.

6. Who we share your personal information with

- Agents and advisers who we use to help run your accounts and services, collect what you owe, and explore new ways of doing business.
- Fraud prevention agencies.
- Companies we have a joint venture or agreement to co-operate with organisations that introduce you to us.
- Companies that we introduce you to.
- Companies you ask us to share your data with.

We may need to share your personal information with other organisations to provide you with the product or service you have chosen:

- If you apply a for maintenance package us, we may pass your personal or business details to the maintenance company.

We may also share your personal information if the make-up of the IFace Group changes in the future:

- We may choose to sell, transfer, or merge parts of our business, or our assets. Or we may seek to acquire other businesses or merge with them.
- During any such process, we may share your data with other parties. We will only do this if they agree to keep your data safe and private.
- If the change to our Group happens, then other parties may use your data in the same way as set out in this notice.

7. How we use your information to make automated decisions

We sometimes use systems to make automated decisions based on personal information we have – or allowed to collect from others – about you or your business. This helps us to make sure our decisions are quick, fair, efficient and correct, based on what we know. These automated decisions can affect the products, services or features we may offer you now or in the future, or the price that we charge you for them.
Here are the types of automated decision we make:

Pricing

We may decide what to charge for some products and services based on what we know.

Tailoring products and services

We may place you in groups with similar customers. These are called customer segments. We use these to study and learn about our customers' needs, and to make decisions based on what we learn. This helps us to design products and services for different customer segments, and to manage our relationships with them.

Detecting fraud

We use your personal information to help decide if your personal or business accounts may be being used for fraud or money-laundering. We may detect that an account is being used in ways that fraudsters work. Or we may notice that an account is being used in a way that is unusual for you or your business. If we think there is a risk of fraud, we may stop activity on the accounts or refuse access to them.

8. Credit Reference Agencies (CRAs)

We carry out credit checks when you apply for a product or services for you or your business. We may use Credit Reference Agencies to help us with this.

If you use our services, from time to time we may also search information that the CRAs have, to help us manage those accounts.

We will share your personal information with CRAs and they will give us information about you. The data we exchange can include:

- Name, Business name and or address
- Account payment and history; and
- Public information, from sources such as the electoral register and Companies House.

We'll use this data to:

- Assess whether you or your business is able to afford to make repayments;
- Make sure what you've told us is true and correct;
- Help detect and prevent fraud
- Trace and recover debts

We will go on sharing your personal information with CRAs for as long as you are a customer. This will include details about your account payments and any debts not fully repaid on time.

When we ask CRAs about you or your business, they will note it on your credit file. This is called a credit search. Other lenders may see this and we may see credit searches from other lenders.

If you apply for a product with someone else, we will link your records with theirs. We will do the same if you tell us that you are in business with other partners or directors.

You should tell them about this before you apply for a product or service. It is important that they know your records will be linked together, and that credit searches may be made on them.

CRAs will also link your records together. These links will stay on your files unless one of you asks the CRAs to break the link. You will normally need to give proof that you no longer have a financial link with each other.

You can find out more about the CRAs on their websites, in the Credit Reference Agency Information Notice. This includes details about:

- Who they are;
- Their role as fraud prevention agencies;
- The data they hold and how they use it;
- How they share personal information;
- How long they can keep data; and
- Your data protection rights.

Main Credit Reference Agencies used are: -

Credit Safe
Call Credit
Equifax
Experian

9. Fraud Prevention Agencies (FPAs)

We may need to confirm your identity before we provide products or services to you or your business. Once you have become a customer of ours, we will also share your personal information as needed to help detect fraud and money-laundering risks. We use Fraud Prevention Agencies to help us with this.

Both we and fraud prevention agencies can only use your personal information if we have a proper reason to do so. It must be needed either for us to obey the law, or for a 'legitimate interest'.

A legitimate interest is when we have a business or commercial reason to use your information. This must not unfairly go against what is right and best for you.

We will use the information to:

- Confirm identities
- Help prevent fraud and money-laundering
- Fulfil any contracts you or your business has with us.

We or an FPA may allow law enforcement agencies to access your personal information. This is to support their duty to detect, investigate, prevent and prosecute crime.

FPAs can keep personal information for different lengths of time. They can keep your data for up to six years if they find a risk of fraud or money-laundering.

The information we use

These are some of the kinds of personal information that we use:

- Name/ Business name
- Registered business address
- Contact details, such as email addresses and phone numbers
- Financial data
- Data relating to your or your businesses products or services
- Data that identifies computers or other devices you use to connect to the internet. This includes your Internet Protocol (IP) address.

Automated decisions for fraud prevention
The information we have for you or your business is made up of what you tell us, and data we collect when you use our services, or from third parties we work with.
We and FPAs may process your personal information in systems that look for fraud by studying patterns in the data. We may find that an account is being used in ways that fraudsters work. Or we may notice that an account is being used in a way that is unusual for you or your business. Either of these could indicate a possible risk of fraud or money-laundering.
How this can affect you
If we or an FPA decide there is a risk of fraud, we may stop activity on the accounts or block access to them. FPAs will also keep a record of the risk that you or your business may pose.
This may result in other organisations refusing to provide you with products or services, or to employ you.
Data transfers out of the EEA
FPAs may send personal information to countries outside the European Economic Area ('EEA'). When they do, there will be a contract in place to make sure the recipient protects the data to the same standard as the EEA. This may include following international frameworks for making data sharing secure.

10. Sending data outside of the EEA

We will only send your data outside of the European Economic Area ('EEA') to:

- Follow your instructions.
- Comply with a legal duty.
- Work with our agents and advisers who we use to help run your accounts and services.

If we do transfer information to our agents or advisers outside of the EEA, we will make sure that it is protected in the same way as if it was being used in the EEA. We'll use one of these safeguards:

- Transfer it to a non-EEA country with privacy laws that give the same protection as the EEA. Learn more on the European Commission Justice website.
- Put in place a contract with the recipient that means they must protect it to the same standards as the EEA. Read more about this here on the European Commission Justice website,
- Transfer it to organisations that are part of Privacy Shield. This is a framework that sets privacy standards for data sent between the US and EU countries. It makes sure those standards are similar to what is used within the EEA. You can find out more about data protection on the European Commission Justice website.

11. If you choose not to give personal information

We may need to collect personal information by law, or under the terms of a contract we have with you.
If you choose not to give us this personal information, it may delay or prevent us from meeting our obligations. It may also mean that we cannot perform services needed to run your products, services or policies. It could mean that we cancel a product or service you have with us.
Any data collection that is optional would be made clear at the point of collection.

12. Marketing

We may use your personal information to tell you about relevant products and offers. This is what we mean when we talk about 'marketing'.
The personal information we have for you is made up of what you tell us, and data we collect when you use our services, or from third parties we work with.
We study this to form a view on what we think you may want or need, or what may be of interest to you. This is how we decide which products, services and offers may be relevant for you.
We can only use your personal information to send you marketing messages if we have either your consent or a 'legitimate interest'. That is when we have a business or commercial reason to use your information. It must not unfairly go against what is right and best for you.
You can ask us to stop sending you marketing messages by contacting us at any time.
We may ask you to confirm or update your choices, if you take out any new products or services with us in future. We will also ask you to do this if there are changes in the law, regulation, or the structure of our business.
If you change your mind you can update your choices at any time by contacting us.

13. How long we keep your personal information

We will keep your personal information for as long as you are a customer of the iFace Group.
After you stop being a customer, we may keep your data for up to 10 years for one of these reasons:

- To respond to any questions or complaints.
- To show that we treated you fairly.
- To maintain records according to rules that apply to us.

We may keep your data for longer than 10 years if we cannot delete it for legal, regulatory or technical reasons. We may also keep it for research or statistical purposes. If we do, we will make sure that your privacy is protected and only use it for those purposes.

14. How to get a copy of your personal information

You can access your personal information we hold by writing to us at this address:

iFace Group Ltd
The Junction,
Charles Street,
Horbury,
WF4 5FH

Letting us know if your personal information is incorrect

You have the right to question any information we have about you that you think is wrong or incomplete. Please contact us if you want to do this. If you do, we will take reasonable steps to check its accuracy and correct it.

15. What if you want us to stop using your personal information?

You have the right to object to our use of your personal information, or to ask us to delete, remove, or stop using your personal information if there is no need for us to keep it. This is known as the 'right to object' and 'right to erasure', or the 'right to be forgotten'.

There may be legal or other official reasons why we need to keep or use your data. But please tell us if you think that we should not be using it.

We may sometimes be able to restrict the use of your data. This means that it can only be used for certain things, such as legal claims or to exercise legal rights. In this situation, we would not use or share your information in other ways while it is restricted.

You can ask us to restrict the use of your personal information if:

- It is not accurate.
- It has been used unlawfully but you don't want us to delete it.
- It not relevant any more, but you want us to keep it for use in legal claims.
- You have already asked us to stop using your data but you are waiting for us to tell you if we are allowed to keep on using it.

If you want to object to how we use your data, or ask us to delete it or restrict how we use it or, please contact us.

16. How to withdraw your consent

You can withdraw your consent at any time. Please contact us if you want to do so.

17. How to complain

If you withdraw your consent, we may not be able to provide certain products or services to you. If this is so, we will tell you.
Please let us know if you are unhappy with how we have used your personal information.
You also have the right to complain to the Information Commissioner's Office.

18. Future formats for sharing data

The Data Privacy laws will change on 25 May 2018. From that date you will have the right to get your personal information from us in a format that can be easily re-used. You can also ask us to pass on your personal information in this format to other organisations.
We are working with our industry to improve the way your data is shared.

19. Cookies

We use cookies and similar technology to distinguish you from other users of our site. We also use cookies and similar technology in our e-mail communications.
This helps us to provide you with a good experience when you use our site or engage in e-mail communication with us and allows us to improve our site and e-mail communication.

A cookie is a small file which asks permission to be placed on your computer's hard drive. Once you or your computer agrees, the file is added, and the cookie helps us analyse website traffic and lets you know when you visit a particular website. Cookies allow web applications to respond to you as an individual. The web application can tailor its operations to your needs, likes and dislikes by gathering and remembering information about your preferences.
A cookie does not give us access to your computer or any information about you, however we are committed to ensuring that your information is secure. In order to prevent unauthorised access or disclosure we have put in place suitable physical, electronic and managerial procedures to safeguard and secure the information we collect online.

We use the following cookies for the following purposes:

- Strictly necessary cookies. These are cookies that are required for the operation of our website. They include, for example, cookies that enable you to log into secure areas of our website.
- Analytical/performance cookies. They allow us to recognise and count the number of visitors and to see how visitors move around our website when they are using it. This helps us to improve the way our website works, for example, by ensuring that users are finding what they are looking for easily.
- Functionality cookies. These are used to recognise you when you return to our website. This enables us to personalise our content for you and remember your preferences.

- Targeting cookies. These cookies record your visit to our website, the pages you have visited and the links you have followed. We will use this information to make our website more relevant to your interests. In some special cases IFace Comms also use cookies provided by trusted third parties. Third party analytics are used to track and measure usage of this site so that we can continue to produce engaging content. These cookies may track things such as how long you spend on one of our websites or pages you visit to help us to understand how we can improve our services for you. IFace Comms also use social media buttons and/or plugins on this site that allow you to connect with your social network in various ways. For these to work, social media sites including Facebook and Google+ will set cookies through our site which may be used to enhance your profile on their site or contribute to the data they hold for various purposes outlined in their respective privacy policies. IFace Comms also use cookies to help us improve our website's usability and for marketing purposes.

We may also use cookies to identify which pages are being used. This helps us analyse data about webpage traffic and improve our website in order to tailor it to customer needs. IFace Comms only use this information for statistical purposes. Google Analytics generates statistical and other information about our websites' use by means of cookies. The information generated relating to our website is used to create reports about the usage of our websites. Google may also store and use this information. Google's privacy policy is available at: http://www.google.com/privacypolicy.html.
If you would like to opt out of being tracked by Google Analytics across all websites please visit: http://tools.google.com/dlpage/gaoptout.
You can block cookies by activating the setting on your browser that allows you to refuse the setting of all or some cookies. However, if you use your browser settings to block all cookies (including essential cookies) you may not be able to access all or parts of our site.
If you would like to find out more about cookies, including how to see what cookies have been set and how to manage and delete them, please visit: http://www.allaboutcookies.org.