



Privacy Policy Template – GDPR Compliant

[This is our bespoke Privacy Policy for our company, Pivotal Marketing Ltd. Feel free to adapt this policy, and our Cookie Policy for your own website, altering them where necessary to inform your website users of examples of when you retain certain information about them, such as contact details, and your reasoning behind this. Alternatively, give us a call on 01484 290100 or email us on solutions@pivotalmarketing.co.uk for a Cookie and Privacy Policy tailored to your needs to suit your company.]

NB This template is a guide and should be amended to suit your business and GDPR legal requirements - Pivotal Marketing do not accept any responsibility for un-adapted use of this template.

[\[REMOVE THE ABOVE SECTION\]](#)

We have created this Privacy Policy to illustrate our strong commitment to privacy, compliance with the GDPR (General Data Protection Regulation) and to show you the policies and practices that we have implemented to protect your personal data. We hope that by doing so, you will feel confident about assigning certain information to us online.

By visiting our website, you are accepting and consenting to the practices described in this policy.

Personal Data We May Collect From You

- **Data you provide us with** - You may give us personal data about yourself when you complete a form on our website or correspond with us by phone, email, social media or post. The personal data you give us may include your name, address, e-mail address and phone number, financial and credit card information.

Why Do We Collect This Personal Data For You

- **For contractual reasons** - to carry out our obligations arising from any contracts entered into between ourselves and you and to provide you with the information, products and services that you request from us.
- **For consensual reasons** - we only keep your personal data if, after sending you this Privacy Policy, you have agreed to us keeping and using your personal data. On the majority of occasions, we will have kept your personal data to provide



you with other useful information about other goods and services we offer that are similar to those that you have already purchased or enquired about. For example, if you have consented, we will use your email address to send you our newsletter providing you with information on tips and latest offers that we believe you will benefit from.

Please note: If you supply us with your business card, for example at a trade show or business event, this is implied consent that you wish our business to contact you. You can withdraw this consent at any time (see the 'Your Rights' section below).

- **To notify you about changes to our service** – our services and practices may change over the course of us having your personal data. If you have consented, we will use your email address to inform you of any changes we believe will affect you or the service you receive from us.

How We Collect Your Personal Data

- We **do not** purchase data from third parties such as databases of email addresses and phone numbers for the purposes of marketing.
- We receive personal data from the information you provide us via the completion of our online forms on our website or correspondence via the phone, email, social media or post with our staff.

How Long We Keep Your Personal Data For

- To comply with the GDPR Data Protection Principle 5, we do not keep personal data for longer than is necessary for the purpose we obtained it for. In practice this means:
 - If you apply for a job at our business but your application is unsuccessful we will permanently delete your personal data from all our systems and devices after 6 months.



- If you are an employee of our business who then leaves the employment of our business, we permanently delete the details of your next of kin from all our systems and devices immediately upon your contract of employment with us ending.
- If you filled out a form on our website or enquired about our service for a quote, but the end result was that you did not use our service, we will permanently delete your personal data from all our systems and devices after 12 months.
- **You are welcome to make a request for us to delete your personal data at any time (see the section titled 'Your Rights' below).**

How We Keep Your Personal Data Safe

Unfortunately, the transmission of information via the internet is not completely secure. However, we take the following steps to ensure the tightest security:

- All information you provide to us is stored on our secure servers.
- Any payment transactions will be encrypted using SSL technology.
- Only the necessary personnel have access to your personal data, to minimise risk.
- Our premises which house our PCs, hard drives and USBs, which can be used to access your Personal Data, are locked overnight and kept secure with appropriate security alarms and measures.
- We use strong, randomly generated passwords, which are changed regularly. We also use two-factor authentication, where a user requires two pieces of information to access personal data we hold. We do not use the same password for different applications. These steps help to keep your personal data that we hold in Cloud-based services, such as our CRM and shared folders such as DropBox, as secure as possible.



Data Breaches:

- In the unfortunate and rare event of a data breach that poses a risk to you, we will inform the Information Commissioner's Office (ICO) and yourself **without due delay and, where feasible, within 72 hours of the breach** to comply with the GDPR. This will give you an opportunity to try and take steps to protect your position, for example, enable you to change passwords and inform your banks that you may be at risk of identity fraud.
- **We are exempt from informing you and the ICO of any data breaches if:**
 - Appropriate technical and organisational procedural measures were applied after a data breach.
 - Subsequent measures were taken to ensure that the high risk no longer exists.
 - The effort to make such a notification would be disproportionate to the risk posed by the breach. This applies when the number of people affected by the data breach is so vast that notifying people on an individual basis within the required 72-hour period is not feasible. For example, if millions of people are affected by the data breach then a press release would be put in the media in place of individual notification to quickly inform everybody affected. This would then be followed up with notifications informing individuals affected but would not have to be within the 72-hour period. Our business would cooperate and work with the ICO in the majority of cases where the data breach is large-scale.

Sharing Your Personal Information

- We will only supply your personal data with our sub-contractors, business partners or suppliers if it is outlined in the written contract we have with you, necessary for us to fulfil our contractual obligations to you and if we have your explicit consent.



- We may disclose your personal data to third parties if we are under a duty to disclose or share your personal data in order to comply with any legal obligation or in the event that we sell or buy any business or assets, in which case we may have to disclose your personal data to the prospective seller or buyer of such business or assets.

Your Rights

Under the GDPR you have the right to:

- be informed about the collection and use of your personal data.
- have access to personal data about you.
- have data about you deleted.
- have information about you corrected.
- object or restrict the Processing of data about you.
- data portability to allow you obtain and reuse your personal data for your own purposes, across different services. This allows you to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability. This enables you to take advantage of applications and services that can use this data to find a better deal for you.
- Rights related to automated individual decision making (making a decision solely by automated means without any human involvement) and profiling (automated processing of personal data to evaluate certain things about you). You can request human intervention or challenge the decisions of automated decision making and profiling.

Due to our business' compliance with GDPR we ensure:

- Once we have verified your identity, we respond to and resolve all Subject Access Requests we receive from you regarding your personal data **within the 30-day time limit of you making the request** as outlined under the GDPR.



- We also **do not charge you any fees** for making a Subject Access Request or for us resolving your Request.
- We send you the information you need to resolve your Subject Access Request in the format that you made the request in. For example, if you emailed us to make your Subject Access Request we will email the required information to you. If you make your Subject Access Request through our Business' Facebook account via Facebook Messenger, we will send you the necessary information via Facebook Messenger.
- We always justify why we cannot comply with your Subject Access Request. For example, if you are enquiring about personal information we had about you but have since deleted due to our 12-month data retention period (see above) we will inform you of this.
- **If Subject Access Requests made by you are deemed to be excessive or unfounded we reserve the right granted to us under GDPR to:**
 - 1) refuse to provide you with the information, always justifying in writing the reasons behind our refusal.
 - 2) charge a reasonable admin fee and again, always justifying in writing the reason for any fees.
 - 3) If your Subject Access Request is particularly complex, for example, we have to go through a large sum of data to access the information necessary to resolve your Subject Access Request, we will write to you within the first 30 days of you making the Subject Access Request and inform you why it will take us longer to comply with your request. Under the GDPR, if we follow these steps, we will have a further 2 months to comply with your Subject Access Request.

Erasing the Personal Data We Have About You



- We will erase any personal data we have about you when you withdraw your consent to us having that data (which you can do at any time), where having the data is no longer necessary and where we can find no legitimate interest for Processing the data any longer.
- **Reserving the rights granted to us under the GDPR and demonstrating our compliance, we will only refuse to erase your data if:**
 - we need your personal data in order to comply with union Member State legal obligations.
 - we require your personal data for the establishment, exercise or defence of legal claims.
 - your personal data is necessary for us to perform a public interest task or exercise official authority.
 - we need your personal data for public health reasons.
 - we require your personal data for archival, research or statistical purposes.
 - your personal data is necessary for us to exercise our right to freedom of expression or information.

In the majority of cases, we will be able to delete the personal data we hold about you if you request us to do so. Where we cannot we will always provide you with justification in writing as to why we cannot comply with your request.