

Ideliver Group Limited



GDPR Policy

Ideliver Group **GDPR**Policy

Contents

Forward

1. What is “Data”?
2. Why do we collect Data?
3. What Data is Collected and How is it Used?
 - 3.1 Data Collected automatically
 - 3.2 Data you provide to us for Sign Up/Sign In
 - 3.3 Data you provide to us for Processing (incl Employee’s)
 - 3.4 Cookies
4. Our Duty of Care and Use Restrictions – Accountability and Governance
 - 4.1 Data processing rights and obligations
 - 4.2 Security and Confidentiality of the Data
 - 4.3 Our Personnel
 - 4.4 Our Technical and Operational safeguarding measures
 - 4.5 Data Protection Officer
 - 4.6 International transfers of Data
 - 4.7 Subcontracting
 - 4.8 Risk Assessments
 - 4.9 Data breaches - Notification
 - 4.10 Record keeping
 - 4.11 Links to Third Party Sites
 - 4.12 Notification of Changes
 - 4.13 Communications
5. Your Rights Under GDPR
 - 5.1 Right to Access the Personal Information We Hold about You
 - 5.2 Right to Rectify Your Data
 - 5.3 Right to Data Portability
 - 5.4 Right to Restrict Processing
 - 5.5 Right to Erasure
 - 5.6 Right to Object

Appendix A - What Data Do We Collect?

- A1) Data Collected Automatically
- A2) Data You Provide to Us for Sign up/Sign in
- A3) Data You Provide to Us for Processing

Appendix B - Our Information Security Policy

- B1) Personnel
- B2) Business continuity and incident management
- B3) Virus and malware protection
- B4) Security monitoring and audit
- B5) Access controls
- B6) Communication, transmission and storage of Data
- B7) Physical and environmental security
- B8) Destruction and deletion of data



Ideliver Group Limited

GDPRPolicy

Forward

Ideliver Group Limited and/or its associated companies and associated trading names is committed to protecting both the privacy of the users of the Ideliver Group website/s, and any of its applications, its customers and suppliers, and all employees and contractors associated with the company, along with the security of any information which its users, customers and suppliers, and all of its employees and contractors associated with the company provide. This privacy policy discloses the ways we collect and manage your data and our compliance with GDPR.

This Policy shall become effective on 25th May 2018 and applies between - Us, Ideliver Group Limited who's Registered Office is: Kemp House 152-160 City Road London EC1V 2NX, (hereinafter referred to as the "Data Processor", "we", "our", "us" "the company"); and - You, the user of our Website and any associated Applications, along with any of our products and services, (hereinafter referred to as "you", "user" "customer" "supplier" "contractor" "employee/s" "staff").

We agree to store, process and/or e-file the Data you voluntarily provide to us

- (a) only as voluntarily and expressly instructed by you within the provisions of this policy
- (b) for the sole purpose of fulfilling the services and products offered by the company
- (c) in accordance with Applicable Law.

This Policy shall be governed by and construed in accordance with English law and the exclusive jurisdiction of the English Courts.

1. What is Data

The GDPR applies to personal data (hereinafter referred to as “Data”) meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data and/or online identifier.

For examples of the kind of Data we may collect, refer to Appendix A.

2. Why do we collect Data?

To supply products and services offered by the company.

Our Website provides the facilities for you to enter your personal details for the purpose of Sign Up and/or requesting a Quotation for the purpose of using our products and/or services, and/or provide and/or supplying such products and/or services as direct result of collecting such data.

To control and manage our staff effectively, calculate company payroll and pension contributions, e-file that information to HMRC and/or any associated pension company, download notices from the HMRC's DPS service, produce payslips, P60, etc, and manage Human Resource services and accounting data online.

By its very nature provision of these services necessitates the collection of personal Data from you.

3. What Data is Collected and How is it Used

Four types of Data may be collected from you.

3.1 Data Collected automatically

We use Data collected automatically to help us to, among other things, administer the Website, help diagnose problems with our servers, track users' web page movements, and to keep the Website up to date and interesting for you as well as comply with our legal obligations.

3.2 Data you provide to us for Sign Up/Sign In

We require personally identifying Data when you sign up with us in order to create a sign in procedure for you to access your account and the data it contains. Once you sign up with our Website and sign in to our services, you are not anonymous to us.

We may on occasion use the email address and other contact details you provided to us on sign up to contact you regarding service orientated issues, for example regarding new services and/or products we offer, how the services and/or products can be used effectively, announcements and/or inviting customer feedback on the services and/or products we provide. We may also use this identifying Data for policing of our users' accounts. We undertake not to send you undue or uninvited marketing email material.

3.3 Data you provide to us for Processing

This data is required in order to provide you with the products and services we offer, human resource management, accounting, e-filing and/or downloading services and/or other services you have signed up to our Website and/or associated Applications for. In addition, you may make use of our Website to store, view, download and/or to print out the data and documents relating to your account, e-filing and downloading.

Data collected may include data about you, our customers, suppliers, employees and/or contractors and their employees. Data is collected by keying in of Data directly into our Websites, or through data interchange technologies e.g. API or SFTP, form filling, or by verbal communications.

Details and an example of what Data is collected is set out in the Appendix A of this Policy. This Appendix will be regularly reviewed and updated to ensure that the contents are accurate and up-to-date.

Privacy by design: We have undertaken to design our Website in such a way to minimise the collection and use of Data. We will advise prior to collection whether the provision of the requested Data is compulsory or whether the information may be provided on a voluntary basis.

Employee's

If you are an employee of the company using our Website and you do not wish to receive emailed or mobile payslips or have access to an online account to view your payslips online you have every right ask Ideliver Group Limited not to enter your email address or mobile phone number into our system. If you already have an online account you can close that account with us forever by clicking on the Close Account option after logging in to your account and following the instructions. Alternatively, you have every right to ask Ideliver Group Limited to remove your email address or mobile number and/or disable your employee account. We use your data to calculate the payroll and pension and transmit the related data on your command to your chosen destination i.e. HMRC, Pension companies, and any third parties you may have chosen e.g. bank.

3.4 Cookies

Cookies are small text files that are placed on your computer, smartphone or other device when you access the internet which enable users to navigate around the Website and (where appropriate) let us tailor the content to fit the needs of our users.

None of the cookies we use collect your Personal Data and they can't be used to identify you. The length of time a cookie stays on your device depends on its type.

We may use three types of Cookie categories

- A. Strictly necessary
- B. Performance
- C. Functionality

A. Strictly necessary

'Strictly necessary' cookies let you move around the Website and use features like secure areas and in some cases online billing. These cookies don't gather any information about you that could be used for marketing or remembering where you've been on the Internet.

We use these to:

- Remember things like information you've entered on forms when you navigate to different pages in a single web browser session
- Identify you as being logged in
- Make sure you connect to the right service on our Website when we make any changes to the way the Website works

We do not use these to:

- Gather information that could be used to advertise products or services to you - Remember your preferences or log in details beyond your current visit

Accepting these cookies is a condition of using our Website, so if you prevent these cookies we cannot guarantee your security or predict how our Website will perform during your visit.

B. Performance

'Performance' cookies collect information about how you use our Website, for example, which pages you visit, and if you experience any errors. These cookies don't collect any information that could identify you – all the information collected is anonymous and is only used to help us improve how our Website works and understand what interests our users.

We use these to:

Provide statistics on how our Website is used

C. Functionality

'Functionality' cookies are used to provide services or to remember settings to improve your visit.

We use these to:

- Remember settings you've applied
- Provide proactive live chat sessions to offer you support
- Show you when you're logged in to the Website
- Share information with partners to provide a service on our Website. The information shared is only to be used to provide the service or function and not for any other purpose

We do not use these to:

- Target you with adverts on other websites

Some of these cookies are managed for us by third parties – where this is the case we don't allow the third party to use the cookies for any purpose other than those listed above.

You can control whether or not these cookies are used, but preventing them may mean we can't offer you some services and will reduce the support we can offer you. It's also possible that preventing these cookies stops us remembering that you didn't want a specific service.

In order to use our Website you must have the cookies enabled on the settings of your device. We use cookies to ensure that we give you the best experience on our Website. If you sign up/sign in to our Website with Cookies enabled in your device setting we will assume that you are happy to receive all cookies from our Website. However, you can change your cookie settings at any time.

4. Our Duty of Care and Use Restrictions under GDPR

Our provisions to promote accountability and governance: As a Data Processor we are fully committed to our duty to safeguard and secure your data. We will treat your data with as much care as if it were our own. Further details relating to our comprehensive Information Security Policies can be found in Appendix B.

4.1 Data processing rights and obligations

We shall process your Data in accordance with the GDPRs, and will not make any use of your Data or allow any use of your Data except as strictly necessary for the purpose of the services and/or products offered by our company and in particular will not use any of the Data for our own or any other commercial purposes.

4.2 Security and Confidentiality of the Data

We shall hold your Data in the strictest confidence and shall not disclose or allow access to the Data or any part of the Data without your prior consent.

We will not disclose the Data to anyone except your intended recipients or if we are required to do so by law or are ordered to do so by a Court.

We shall restrict access to your Data by our own Personnel - access will be limited to only those Personnel that are required to have access to the Data for the purpose of providing the services offered.

4.3 Our Personnel

We shall ensure that our Personnel:

- are reliable and fit and proper persons to have access to your Data
- are informed of the confidential nature of the Data and are bound by contractual or statutory confidentiality obligations in relation to the Data; and
- have received appropriate, regular and recent training and guidance on data protection and security.

4.4 Our Technical and Operational safeguarding measures

We shall:

- implement and maintain appropriate technical and organisational measures to prevent the accidental, unauthorised or unlawful processing, destruction, loss, alteration, damage to or disclosure of, or access to, your Data.
- ensure that the technical and organisational measures implemented are appropriate to the risks presented by its processing of the Data, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons and the harm that might result from the accidental, unauthorised or unlawful processing, destruction, loss, alteration, damage to or disclosure of, or access to, the Data; and
- regularly review and update the technical and organisational measures implemented.
- maintain a fully resourced and funded Data Protection Officer.

4.5 Data Protection Officer

Our Data Protection Officer's minimum tasks will be:

- To inform and advise our personnel about their obligations to comply with the GDPR and other data protection laws.
- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train personnel and conduct internal audits.
- To be the first point of contact for individuals whose data is processed (employers, employees, clients, etc) and report directly to the board of Directors.

4.6 International transfers of Data

We may have reason to transfer and/or share some or all of your supplied data outside of the European Economic Area (EEA), the European Union (EU) or the UK, for the purpose of supplying your requested quotations products and/or services.

We shall not transfer your Data outside the European Economic Area (EEA), the European Union (EU) or the UK without your prior knowledge and/or prior written consent.

4.7 Sub-contracting

We shall not, without your knowledge, allow any third party sub-contractor to process your Data. In the event that you do provide written consent to processing of the Data by a third party, we shall to the best of our abilities ensure that the third party has implemented and maintained technical and organisational means to prevent unauthorised or unlawful processing of or accidental loss of or destruction of the Data.

4.8 Risk Assessments

We will conduct regular Data Privacy Impact Assessments (DPIAs) to identify and assess reasonably foreseeable internal and external risks to the security, confidentiality and integrity of electronic, paper, and other records containing Data and evaluate and improve, where necessary, the effectiveness of its safeguards for limiting such risks.

4.9 Data breaches - Notification

We shall notify you without undue delay and within 72 hours if we become aware of any actual breach or reasonable grounds for suspicion of a Data breach including without limitation any actual or suspected personal data breach affecting the Data.

We shall include in our notification:

- a description of the nature of the breach
- the details of our contact who can provide further information about the breach;
- a description of the likely consequences of the breach,
- a description of the initial remedial measures taken or proposed to be taken to address the breach,

4.10 Record keeping

We shall keep records of the processing of the Data and all information necessary to demonstrate our compliance with the GDPRs. We shall on reasonable notice make available on request all information necessary to demonstrate compliance with GDPR obligations.

4.11 Links to Third Party Websites

Our Website may provide links for you to access third party websites only as a convenience and the inclusion of any link does not imply our endorsement of that particular website. You are responsible for viewing and abiding by the respective privacy statements and terms of use posted on any linked sites. We accept no liability for the privacy practices or content of websites that may be linked to from our Website. This privacy statement applies solely to information collected by our us and/or our website.

4.12 Notification of Changes

We may update this GDPR Policy to reflect changes to data protection practices. If any material changes are made a prominent change notification will be displayed on our Website prior to the change becoming effective. You should review this page for the latest information on our privacy practices each time you visit our website.

4.13 Communications

If we receive any complaint, notice or communication which relates directly to the processing of the Data or to either our or your compliance with the Data Protection Laws, we shall immediately notify you and where necessary provide you with assistance in relation to any such complaint, notice or communication.

5. Your Rights Under GDPR

5.1 Right to Access the Personal Information We Hold about You

In accordance with Applicable Law, you have the right to access the Data we hold about you. You can do this at any time by signing in to your account on our Website and viewing the data in your account or requesting that the company system administrator discloses

the material facts to you. For security reasons we may also ask you to further verify your identity and to provide more details about your request.

5.2 Right to Rectify Your Data

It is your responsibility to ensure that you submit true, accurate and complete information to us. By signing in to your account you have the facilities to review any data which you upload or entered to our Website and to make changes to any data prior to it being e-filed.

Employee's

Any modification of data must be carried out by the System Administrator or any Additional Users appointed by the System Administrator at their sole discretion. Please be aware that after Data has been e-filed to HMRC for the purpose of payroll procedures, it is not possible to amend that Data.

5.3 Right to Data Portability

You have the right to download your Data from our Website at any time. To do so sign in to your account, or requesting that the company system administrator discloses the material facts to you.

5.4 Right to Restrict Processing

When you pass us your data through the by uploading or entering your data directly to our Website, your data will only be processed in accordance with the purpose of which your data has been supplied to us, you can restrict the processing of your data at any time by contacting us through the member portal, or by our email info@idelivergroup.com.

5.5 Right to Erasure/Closure of your Member Account/'Right to be Forgotten'

You have the right to close your account with us at any time. If you do this you will no longer be able to access your data.

Employees

At the moment we are legally obliged to retain your Data for a minimum period of six years as required and stipulated by HMRC policy for tax record purposes. It cannot be deleted during this period. After the minimum period the data can be deleted from our system on request. HMRC are yet to publish their detailed policy on data deletion. As soon as they do we will update our policy and practices accordingly to comply.

5.6 Right to Object

If you have any questions of concerns about this GDPR Policy and/or our practices regarding Data Protection , or would like to exercise your rights in relation to your Data, please contact our Data Protection Officer at info@idelivergroup.com, or write to: The Data Protection Officer, Ideliver Group Limited, Unit 805 Fowler Road, Oakwood Business

Park, Clacton-On-Sea Essex CO15. To ensure your correspondence reaches us you undertake to send it to us by recorded delivery post.

If you have a complaint or concern about how we are processing your Data we will endeavour to address such concern(s). However, if you would like to direct your complaint/concerns to a Data Protection Authority, the contact details for your local Data Protection Authority are as follows: <https://ico.org.uk/global/contact-us/> (<https://ico.org.uk/global/contact-us/>).

Appendix A

What Data Do We Collect?

Further details of the Data being processed and the nature and the purpose of the processing.

A1) Data Collected Automatically

Whenever you visit or interact with the Website, we may use a variety of technologies that automatically or passively collect information about how the Website is accessed and used. The Personal Data collected is used to improve the appropriateness of the services provided on the Website.

Data collected automatically may include:

- IP address or other unique identifier for the computer, mobile phone, tablet or other device you use to access the Website
- Device type
- Demographics
- Location
- Language
- Type of browser software and operating system you are using
- Page(s) served, the time, and the preceding page views
- Event type (pages viewed/documents downloaded)
- Event date/time
- Page URL
- Downloaded item URL
- Email address
- Organisation type (access permissions)
- Organisation name
- Telephone number
- Date of form submission

A2) Data You Provide to Us for Sign up/Sign in

We will collect personally identifying information when you sign up in order to create a sign in to account function. We will ask for your full name, address, e-mail address, and other information we may decide upon from time to time.

Appendix B

Our Information Security Policy

As a Data Processor we have a responsibility for promoting good practice in information security across our organisation and for monitoring the effectiveness of information security.

Our information security policy is summarised below:

We require that:

- that any confidential information shall when not in use be placed in a secure location and the imposition of a 'clear desk' policy; and
- personnel to log-on/log-off of computer systems when entering or leaving a terminal/workstation.

B1) Personnel

We shall:

- ensure that Personnel who have access to the Data are authorised prior to commencing work to ensure that they are reliable and fit and proper persons to have access to the Data;
- adequately train Personnel on data protection and security;
- ensure that Personnel understand their obligations to keep the Data secure and confidential;
- ensure that Personnel have committed themselves to binding confidentiality obligations;
- ensure segregation of duties for critical and sensitive roles and reduce reliance on key individuals; and,

B2) Business continuity and incident management

We shall:

- define procedures for dealing with incidents including without limitation investigation, planning of remedial action, resolution, communications, supervising activity and documenting actions taken;
- have business continuity strategies and processes/ disaster recovery plans including (without limitation) the ability to restore the availability of and access to the Data in a timely manner in the event of a physical or technical incident; and
- regularly back-up copies of the Data stored securely and separately from the live files.

B3) Virus and malware protection

We shall:

- have in place industry recognised virus and malware protection software and techniques to prevent infection by viruses and malware.
- maintain the use of automatic update mechanisms for anti-virus software.
- Regularly review the software and data content of systems supporting critical business processes and the presence of any unapproved files or unauthorised amendments shall be formally investigated.

B4) Security monitoring and audit

We shall:

- have a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in place for ensuring the security of the processing of the Data;
- have the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; and
- shall regularly carry out monitoring, testing and audits of the measures in place to keep the Data secure and confidential and make improvements based on the recommendations coming out of such monitoring, testing and audits.

B5) Access controls

We shall ensure that we have in place procedures that control access to files, documents and systems containing the Data. We shall ensure that the access control arrangements:

- cover access by all Personnel including without limitation, business users, individuals running the system and specialist IT staff, such as technical support staff;
- include password controlled access to systems
- restrict access to the Data in line with access control policies;

B6) Communication, transmission and storage of Data

We shall:

- use encryption as appropriate when the Data is in transit and at rest;
- not use, reproduce or store any of the Data on an externally accessible computer or electronic information retrieval system; and
- implement controls to prevent the Data being sent to or access by unauthorised parties.

B7) Physical and environmental security

We shall control access to facilities where Data is processed and have in place adequate precautions against unauthorised access by:

- fitting intruder alarms and locks;
- recording the arrival / departure of visitors and supervising them at all times;
- providing CCTV surveillance

B8) Destruction and deletion of data

We shall as necessary implement appropriate measures to securely destroy and permanently delete files and documents containing the Data.