General Data Protection Regulation (GDPR)

a. General Data Protection

i. At Woody's Express, we aim to promote high standards in the handling of personal information and so protect every individual's right to privacy.

ii. All data is;

1. Fairly and lawfully processed,
2. Processed for specified purposes,
3. Adequate, relevant, and not excessive,
4. Not kept for longer than is necessary,
5. Kept up to date,
6. Processed in line with the rights of the individual,
7. Kept secure,
8. Not used for outside marketing purposes
9. Not transferred to any outside bodies (including marketing), with the exception of;
    a. Our accountancy firm – CIB Services
    b. Any subcontractors involved in the transaction, such as DHL or FedEx.
    c. Any government bodies which request data by law, such as HMRC.

b. IT systems compliance

i. Data controller

1. As Woody's Express is a small business, the overall data controller will be the IT Manager and System's Administrator. The current IT Manager/System Administrator is Donald Sansom, and can be contacted at donald@woodys-express.com or 01851701988
2. Account holders are managed by Murdo Macphail, the Accounts Manager.

ii. Data processor

1. Currently we process data through a content management system (CMS) which was designed by Donald Sansom the System's Administrator.
2. The CMS is the Woody's Web Portal, currently on version 2.0. The CMS is currently hosted with 1and1 cloud hosting on servers in the US, backed up across to Dataflame cloud hosing in the UK, and mirrored in-house on a Dell Poweredge Debian web hosting server.
3. For accounts data processing, we have a Dell Poweredge T420 Windows SBS 2011 Server running Sage Accounts 50 2015.

c. Employee awareness

i. By May 28th 2018 we aim to have all data collecting staff fully trained on GDPR. This includes, but is not limited to, administration staff who work at reception and take bookings by telephone, email, and in person.

ii. When data is collected by an employee in relation to a customer, employees will make customers aware that their personal data will be stored on our content management system for up to a year to comply with our ISO9001 certification.

iii. Employees taking information from a customer should give them the choice if they wish their personal data to be held. If not, the data will be automatically erased after 30 days.

d. Information we hold

- **i.** Registrants to our website
  1. Customer data is held when an account is created on our website. This data is held with the customer's permission and includes;
     a. Contact Name
     b. Address
     c. Telephone Number
     d. Email Address
- **ii.** Business web portal account holders
  1. Client data is held for each account opened for access to our content management system. This currently includes;
     a. Contact Name
     b. Company Name
     c. Address
     d. Telephone Number
     e. Email Address
- **iii.** Account holders on the Sage 50 accounts invoicing system
  1. Account holder data on the Sage 50 system held includes;
     a. Business Name
     b. Contact Name
     c. Telephone Number
     d. Mobile Number
     e. Address
     f. Email Address
     g. Website Address
     h. Amounts outstanding
     i. Amounts paid
  2. Invoice data includes
     a. Details regarding services used such as products shipped
     b. Consignee and Consignor data
     c. Cost of services
- **iv.** Consignee & Consignor data relating to a consignment
  1. Consignee & Consignor data is collected at point of sale.
  2. This data is stored on our content management system for any queries relating to collection or delivery of a consignment.
- **v.** Data held on both the Consignee & Consignor is;
  1. Contact Name or Company Name
  2. Full Address
  3. Landline Telephone Number
  4. Mobile Telephone Number
  5. Email Address
  6. Any Special Instructions relating to collection or delivery point
  7. Products that are to be handled
  8. Any Reference or Order Numbers
- **vi.** Information passed to us from a subcontractor for a delivery or collection

1. Subcontractors may pass paperwork along with an item for delivery. This paperwork may include but is not limited to;
    a. Customer Name
    b. Customer Address
    c. Customer Telephone Number
    d. Customer Email Address
2. Paperwork passed to us by a subcontractor is usually passed to us to obtain a signature from the consignee and to be returned to the subcontractor.
    a. A copy of this paperwork is kept on our server in case of the event of a delivery dispute for up to 1 year, unless the subcontractor's customer has requested erasure under GDPR.
    b. We expect subcontractors to follow the guidelines set out by the GDPR and notify customers that their personal data will be held and offer them the same choice we do to have that information held or erased.

e. Data flow & Data sharing

i. Accountancy Firm
    1. Our accounts data is shared with the CIB Services accountancy firm, who audit and monitor our accounts and cash flow.

ii. Subcontractors
    1. If a subcontractor is required to complete a shipment, customer data may be passed to the subcontractor used in the transaction.
    2. Customers will be made aware of any transfer of personal data at the point of sale, and to which subcontractor it is being transferred to.
    3. Customers will be given the right to request erasure of that data once the subcontractor has completed the delivery on our behalf.
    4. Subcontractors will be notified if the customer has requested their personal data to be erased.

f. Data Accuracies & Potential Inaccuracies

i. When collecting data from customers, staff are expected to ensure that data is recorded accurately in the content management system.

ii. If customers create an account on our website, the data held on the content management system will reflect that entered in the registration form by the customer.

iii. Customers have the right to request correction of potential inaccuracies held on our systems, and those inaccuracies must be forwarded to shared parties such as subcontractors or accountancy firms.

g. Communicating privacy information

i. Privacy notice in plain English
    1. A new privacy notice has been created in compliance with the GDPR
    2. The privacy notice will be in plain English and easy to understand
    3. The privacy notice will communicate to the public;
        a. How customer data is used

b. Where customer data is passed to
c. If customer data is used for any marketing purposes
d. Data retention periods
e. Legal basis for processing the data
f. Where a person can complain to regarding data processing

ii. Easy access

1. The privacy notice is easily accessible via our website on http://woodys-express.com/privacy
2. For persons who do not have internet access, a copy can be obtained free of charge from our offices
3. For persons living out with the locality of our offices, they can request a copy be sent to them, free of charge, by phoning our head office on 01851703908.

h. How customer & client data is used

i. Retention periods

1. Personal/Business data, for those who registered with our web service, or business portal, will be retained for usage when shipping consignments. This registration data will be retained until that person or business requests their account to be closed and/or erased.
2. Consignee and Consignor data relating to each consignment will be retained for 1 year in line with our ISO9001 certification, unless that person wishes for their data to be removed from our system, either after 30 days from point of entry, or under the GDPR right to erasure clause.
3. Transactional data involving finance must be kept for at least 5 years in accordance with HMRC guidelines.

ii. Legal basis for processing the data

1. Contractual necessity

a. Quotations, Collections, Deliveries & Payments
    i. When a customer requests a quotation, collection or delivery, either by phone, email, in person, through their online web account, or other means, they are entering into a contract with the company to carry out their request. This gives the company a legal basis for processing their data to fulfil the request.
b. By registration on our website
    i. Registering as a customer on our website, gives the company legal basis for processing their data and storing their data as a record with acceptance of our privacy policy.
c. Over the phone
    i. As stated in paragraph A of this section, when a customer requests Woody's Express to fulfil a request on their behalf, they are giving the company legal basis for processing the data.
d. Businesses using our web portal
    i. Businesses registered online on our content management system are giving us the legal basis for processing data entered in to the system when filing a request for a collection or delivery. It is necessary for us to process the data to fulfil their request.
e. Data received via email

i. Data received via email is used to process and handle a customer's query and/or request. The data received may need to be queried to other departments to answer a question or fulfil a request.

2. Consent

a. Personal data may be processed on the basis that the data subject has consented to such processing.

b. Consent will be requested from the individual for processing, passing, and holding of the customers data.

i. Individuals' rights

i. Subject access rights

1. Individuals have the right to access any data held on them by the company at any time.

2. They may request to see what data has been held on them by the company and for how long.

3. The company will be fair and transparent when handling these requests.

ii. Rights to have inaccuracies corrected

1. Individuals have the right to have any inaccuracies corrected.

2. Inaccuracies must also be communicated to any third parties for correction.

iii. Right to erasure

1. Individuals have the right to erasure, this gives them the right to have all personal data removed on our system.

iv. Right to prevent direct marketing

1. Individuals have the right to prevent direct marketing under the GDPR.

2. Woody's Express offers individuals the option to take part in direct marketing when registering on the company's website, rather than offering to opt-out.

v. Right to prevent automated decision making & profiling

1. Woody's Express does not make automated decisions or profiling.

vi. Right to data portability

1. Individuals have the right to receive a copy of their data in a format friendly to them.

2. Woody's Express offers data portability in CSV file format or Excel format.

vii. Contact Personnel

1. Woody's Express IT Manager will be able to assist in Subject Access

2. Donald Sansom
Head Office, Rigs Road, Stornoway, HS1 2RF
donald@woodys-express.com
01851701988

j. Subject access requests

i. Cost for data

1. There will be no charge for access to data, or exportation of data.

ii. Timescale

1. Access requests will be addressed within the 30 day timescale outlined in the GDPR

iii. Right to refusal

1. Woody's Express has the right to refuse subject access when the request is manifestly unfounded.

k. Consent

i. Consent to hold customer data must be recorded. Internal auditing will be conducted to ensure that consent is being communicated and customer's consent is being received and documented for data storage.

ii. There are two types of consent
   1. Unambiguous consent
      a. Woody's Express must be able to demonstrate that we have had the customer's authority to record their data.
   2. Explicit consent
      a. Explicit consent requires a subject to clearly and explicitly agree to their personal data being processed.

iii. Children
   1. Woody's Express does not allow registrations anywhere or transactions of persons under the age of 16.

l. Data breaches

i. Reporting to the Information Commissioner's Office
   1. Data breaches will be reported to the ICO if it is likely to result in a risk to people's rights and freedoms (i.e. identity theft).

ii. Notifying individuals
   1. All individuals will be notified if there is a data breach, and the potential impact it could have on them. Advice will be given on how to minimize the impact of the breach.

iii. Notifying clients that have connected/integrated systems
   1. Clients will be notified immediately if there is a breach any potential risk to their network or systems. Any integrated systems will be immediately disconnected if there is a breach found at Woody's Express. This will be done to minimize any risk or impact on clients which are connected to our systems.

iv. How data breaches are managed
   1. Assessing the breach
      a. The breach will be assessed by the management team.
      b. The scale and impact of the breach will be assessed.
      c. Areas will be assessed as to which have been breached. i.e. whether the it is a single workstation, the accounts management server, or the entire network and content management system.
   2. Key personnel
      a. Donald Sansom – IT Manager
      b. Jori Kim – Office Manager
      c. Murdo MacPhail – Accounts Manager
      d. Danny Richardson – IT Consultant
   3. Damage limitation

a. Protect other parts of the company and disconnect them from the network.
b. Any outside integrated systems will be immediately disconnected.
c. Any internal systems will be disconnected from the network until the breach has been properly identified.
d. Isolating the infected system/breach as quickly as possible.

v. How data breaches are documented
   1. Data breaches should be documented by the IT Manager in a readable format for future reference.
   2. Details should be in plain English and not IT Jargon as to what happened so other employees can understand what happened.

vi. How it can be prevented in the future
   1. Details of how it can be prevented in the future should be documented by the IT Manager.
   2. Any security updates, patches, and extra protocols that can be implemented to prevent future breaches must be done as soon as possible.

m. Data protection by design

i. Privacy by design
   1. GDPR advises privacy by design, and from the writing of this document, privacy will be at the forefront of any future software development within the company.
   2. Any modifications to the content management system or web site will use the privacy by design approach.
   3. Privacy by design is considered the best approach by Woody's Express as consumer privacy is thought about first before implementation or development of any software.

ii. Privacy impact assessment
   1. Woody's Express is in the process of developing its own privacy impact assessment screening questionnaire to assess risks and impacts of customer data storage.
   2. This screening questionnaire will be used when designing any future applications for the company to ensure GDPR standards are met.

n. Data protection officer

i. As Woody's Express is a small business the DPO will be default to Donald Sansom – IT Manager
ii. His contact details are donald@woodys-express.com and tel: 01851701988

o. International

i. We do not currently hold any business premises out with the UK. However we do conduct international shipments and customer data is sent to subcontractors.
ii. We expect subcontractor to adhere to GDPR standards the same as Woody's Express, whether they are in the EU or outside.