Introduction

Parcelhub Limited holds personal data relating to its employees and clients, and also to business contacts for the purposes of marketing the business. We are a Data Controller of this data, and this policy itemises the legitimate bases for our holding, processing and retention thereof, together with how it is used and protected.
In addition we use and transfer address data (including personal data), supplied by our clients, pursuant of our business offering of providing a multi-carrier label-generation platform, and for the purpose of despatching items that we have stored and/or packed and prepared for despatch to given addresses. We are a Data Processor of this data, and this policy includes the details of how it is processed and retained, such that may be included in the policies of the ultimate Controllers of the data that is processed through our systems. The pertinent elements of those details are also included in the Contractual Agreements made available to our clients regarding our processing of their data.

Parcelhub Limited is registered with the ICO, registration number ZA308498.

Our Personnel and Human Resources Data

We collect the following details from employees at the start of or during their employment and provide them to Whistl Limited by secure data transfer:

- name and address,
- proof of identification and right-to-work
- past employment and qualifications,
- details necessary for payment, including proof of bank account,
- nominated next-of-kin,
- details of disabilities and health conditions on a voluntary basis,
- performance records, incapacity and attendance records,
- training records during employment.

Whistl Limited are a Controller of this data and it is held by them according to their own policy.

After providing data to Whistl, we retain a single record (secured in files of restricted access) of this for up to three months prior to deletion. Other than this we only retain information as outlined below.

We retain a record of the names, positions held, and dates of service of past and present employees. Consent is requested from the individual in question before these are provided to other third parties.

We hold name and address details and contact details for employees during their employment and for a period of 2 months thereafter in order to fulfil their Contract of employment.

We hold the details of a nominated next-of-kin or other person for each member of staff by their Consent, as a point of emergency contact during the period of their employment only.

We hold records of employee training records during their employment on the basis of our Legitimate Interests of confirming the safe usage of equipment and processes.

We hold details of any disability or other condition that an employee chooses to make us aware of as significant in the way their role is managed or in the way they may need to be treated by a first-aider on a Consent and possible Vital Interests basis. This Special Category data is held only during the period of employment and shared only according to the wishes of the employee.

Our Communications and Recordings

We retain CCTV recordings of activity within our warehouse and despatch areas, and the entrances and exits to all of our premises, for 6 weeks prior to deletion. Access to recordings is password-protected and available only on a highly restricted basis. These may contain identifiable images of our employees, of sub-contractors working on our premises, of visitors, and of individuals collecting or delivering goods. Recordings are retained for the Legitimate Interests of our business identifying criminal activity, identifying and remedying activity that may present risks to safety, and validating the nature, timing, and contents of disputed deliveries or collections. A longer-term recording may be kept of any such activity identified. The balancing risks to the rights of our employees are considered negligible in that they are aware of being recorded and should have no reason for concern about their working activities being seen, and in that the recordings are not used except as itemised above. While non-employees will not necessarily be aware that they are being recorded and this is to be considered in assessing their rights, the restricted use and short storage-period of the footage adequately limits any risk to those.

We retain recordings of all telephone communications for 30 days prior to deletion. These may contain information that personally identifies either a caller or others. A recorded message informs external callers that recordings are being made for “training and quality control” reasons. Access to recordings is restricted to administrators of the system (granted only by validated request) and to quality controllers. Recordings are retained in our Legitimate Interests of monitoring employee performance in this area and of investigating complaints over the verbal statements or manner of our employees, and to verify the existence or agreement of formal business arrangements, and are not used for other purposes. A longer-term recording may be kept of any such complaint validated or still under investigation. As all participants in the telephone communication are aware that it is recorded and for what purposes and the retention period is short, those purposes present no clear risk to anyone’s rights.

We retain records of all email communications for up to 2 years, and also archive those on Mimecast (a cloud-based cybersecurity system) for 7 years before permanent deletion. These may contain personal data; our staff data policy stipulates that including such information in emails should be restricted wherever possible especially with regard to personnel matters, and our contractual agreements with customers make clear that submitting lists of addresses in this way is not advised. Emails are accessible to the sender and receiver, to an immediate line-manager in some cases, and to system administrators. Emails are retained on a Legitimate Interests basis, primarily due to the importance of keeping supplier and client communication discussing and agreeing terms and costs of business that may not be otherwise available. The balancing risks to the rights of individuals are limited by the restriction of inclusion of personnel matters, and therefore significant personal data, in email communications; it is considered that the presence of the names of senders and recipients of business communications presents no obvious risk to their rights.

Our Client, Sales and Marketing Data

We hold contact details for nominated representatives of our clients in order to communicate with them regarding their account and our services, and in order to provide support for parcels despatched through our systems. A line of communication is required for Contract reasons and additional contact details are added on a Consent basis. These details are also shared with other entities within the Whistl Group and thereafter held and used according to their own policy.

Details of financial or contractual arrangements with our clients (contracts, sales agreements, and account set-up forms), which may contain personal data limited to contact names and signatures, are retained for a period of 7 years on the basis of Legal Obligation relating to the possible requirements of HMRC.

We may retain the contact details of former customers and of enquirers about our services for up to 2 years after last communication on the basis of our Legitimate Interests of marketing our business by informing them of the services provided by the Whistl Group in addition to the services they have previously used or enquired about. This will include the transmission of our emailed newsletter, containing news of interest to current and potential customers about our business and services. Receivers of our newsletter can contact us to unsubscribe from this list or do so by clicking the 'Unsubscribe' button received in all such communications after which they will receive no further such transmissions. Restricted communication, targeted to a proven area of interest, to a business contact presents only a highly limited risk to their rights.

We may source lists of targeted business contact data from other companies in the Legitimate Interests of marketing our business. Those lists will only relate to companies likely to be interested in services related to ours. No subsequent contact will be made with any contact that has chosen at any previous time not to be contacted by us. Restricted communication, targeted to a likely area of interest, to a business contact presents only a highly limited risk to their rights.

We use MailChimp, a US-based operation to provide email marketing communications. Our use of MailChimp has been covered by a transfer risk assessment validating this transfer of data outside the EEA as not of a high risk level, due to the limited personal data involved and the adequacy of MailChimp's security processes.

Data Processed for our Clients

We process data on behalf of our clients by using their submission through the Parcelhub software and/or website to supply relevant information to providers of courier and postal despatch. In addition, we process data by receiving and formatting supplied information such that it is suitable for entry into any relevant despatch systems, and by using that information to produce and print despatch documentation. This data may be submitted to us by clients for processing by file transfer, email or telephone communication, or by extraction from a website. We process the data for the purpose of enabling delivery to our client's designated recipients.

These submissions may contain a number of types of personal data, frequently consisting of name and address information and sometimes also accompanying telephone numbers and/or email addresses. Those names may be connected with either business or home addresses, and their usage for both business and personal purposes. While it is conceivable there may be personal data relating to vulnerable persons, to children, and to other special categories of person within the data, this in current practice will not be identifiable therein, nor is the purpose of processing related to that status.

We retain files within which data is submitted outside the Parcelhub system for a period of 30 days following last processing, after which they are deleted.

Data processed for courier despatch is retained for a period of 90 days following despatch within both our and Whistl's central courier databases, prior to its anonymisation by the removal of any identifiable personalising information. Clients can elect to hold address information within their control in the Parcelhub software or website for a longer period by saving it as part of the designated 'address book' – this is the only exclusion from the anonymisation process.

During its retention period, elements of the processed data are accessible to our staff for the purposes of investigating despatch, verifying charges made to us, and other related purposes. Use and retention of that data remains governed by this policy. Restricted staff of other companies within the Whistl Group also have access to this data, and are bound by the law not to use, view or extract the data in ways outside its original purpose or those outlined in this policy.

We submit data to the supplier of the chosen despatch service for the purpose of conducting delivery, where it will then be stored by that supplier in line with their own processing terms – the choice of despatch supplier to sub-process their data belongs to our clients and is transparent to them. We have verified that the practices and policies of these suppliers are compliant with GDPR.

Periodically the security of our systems is verified by penetration testing, conducted by a verified UK-based external security consultant. This process is governed by agreement and consists of only temporary possible access to data and an assurance of no extraction.

If data is processed using our stock/warehouse management system, it is stored therein for a period of 6 months prior to anonymisation by removal of personally-identifying name and address details.

Data supplied to us by couriers in support of their invoices to us will in some cases contain personal data. We anonymise this data by removing personalising elements on receipt and before processing or storing it otherwise.

Subsequent to despatch, our clients may raise queries about the delivery process, or our employees may notify clients of delivery problems. These may be handled either by our staff, by supporting staff of other companies within the Whistl Group, or by other companies including those that may process data outside the UK. Communications resulting from this, which may contain personal data, are recorded within a ticketing system. This information is anonymised 30 days after the conclusion of the process. In cases of a claim being made for compensation over a delivery failing, clients may submit to us information from the parcel recipient in support of the claim containing personal data. This is passed to the courier in line with their stipulation and then anonymised in our records.

On request, we sometimes obtain and provide proofs of delivery for our clients, consisting of a recipient signature linked to a delivery address. We do not store this information after submission for longer than a period of 1 week.

Undelivered parcels or postal items may be returned to our premises by the despatch provider with personal data visible on the outer labelling. These are either returned to our clients or, if held on our premises otherwise or ultimately destroyed, the personalising element such as label or envelope is shredded and then recycled. If such items are returned to our clients we may obtain and store for 90 days a signature confirming receipt thereof.

Our stated policy is that there should be no reason for a client to supply definable Special Category data to us for the purposes of its processing. It is possible that in certain specific instances the supply of a product description in combination with personally identifiable details will constitute Special Category data (such as indications within the data submitted that link a named recipient to a particular type of parcel or despatching company in a way that defines their beliefs, health, race, or the like). The responsibility for legal processing of this data, which will normally involve obtaining and recording explicit consent for all processing from the data subject, rests with our client. Should there be no alternative to the client supplying Special Category data to meet its processing deeds, we require a Variation of Terms to be agreed specifying that they meet their legal processing requirements.

Information, which may include personal data, that is submitted to or by us by email is stored therein for a period of 2 years after submission and also archived on Mimecast (a cloud-based cybersecurity system) for 7 years before permanent deletion. Secure forms of information transmission other than email, deleted within 30 days of use, are alternatively available to clients that do not have their own such method in place.

Data Subject Requests

GDPR provides a number of specific rights to data subjects:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

We treat our responsibilities under the regulation with respect and comply fully with these rights.

If a data subject makes a request of us in relation to one of these rights, in the first instance we request supply of proof of identity in two forms: an identifying document such as a passport or driving licence, and a utility bill or similar proof of address. We also ask for an indication of why they believe we hold their data (e.g. the type of parcel or communication they have received) to assist with identification of where their data is held.

In cases where the data involved is processed on behalf of a client, we will communicate this to the data subject, comply with the request in relation to any data held by us, and also pass on the request to the client and ultimate Data Controller to take any necessary action.

We will comply with all such requests as soon as possible, and within one month of proof of identification. In most cases it will be possible to comply immediately.

We do not plan to charge for compliance with any such requests, nor to consider refusal or extension of the one month time period for compliance, but we reserve our right under GDPR to take such action of this type as is reasonable and proportionate in a case where a request is manifestly unfounded, excessive, or repetitive.

Personal Data Breaches

A personal data breach is defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Should we become, or be made, aware of such a breach, it should be reported to our Data Protection Officer without delay.

In the case of a breach relating to data of which we are the Data Controller, an assessment will be made of the likely risks to the rights of the individuals involved. Based on that assessment, the required notifications will be made to either or both of the ICO and the data subject(s). The assessment and also, where possible, any notifications will be made within 72 hours of awareness of the breach, or in the case of data sourced via Amazon integration, to 3p-security@amazon.com within 24 hours.

In the case of a breach relating to a client's data of which we are the Data Processor, the client will be made fully aware of the circumstances, nature and possible impact of the breach within 72 hours. If required, we will also advise on the level of the breach and the types of notifications the Data Controller is required to make.

Organisational Security Processes and Transfer Policies

We keep personal data secure against loss or misuse. If other organisations outside the Whistl Group process personal data as a service on our behalf, we will verify their security arrangements and compliance with GDPR.

In cases where our personnel data is stored on printed paper, it is kept in a secure and locked container where unauthorised personnel cannot access it. Printed data is securely shredded when it is no longer needed.

Our computers are protected by strong passwords that are changed regularly – we enforce a 90 day password change and a minimum 8 characters with three of the four levels of complexity included. After 5 minutes without use screens are automatically locked requiring passwords to unlock, and our staff policy dictates that all screens should be locked when employees leave them unattended.

Our servers containing personal data are kept in a secure location, locked and keycoded and accessible only to select authorised staff. Data is also transmitted via the Whistl Group's SFTP servers. All servers containing data are protected by security software and firewall.

Any NAS device used in conjunction with local PC backups is placed inside our locked server room. We restrict, via our application control and application control software, the use of external drives, flash drives, and the download of any software by staff members. Our policy restricts the saving of any data directly to mobile devices such as laptops, tablets or smartphones.

Data is regularly backed up within its own server and stored there for 1 day. Data is also backed up to Microsoft Azure Backup Server for a period of 30 days, accessible only to restricted senior staff and system administrators.

There are restrictions on transfers of international data. The only transfer of our own data outside the UK or EU (and hence the jurisdiction of GDPR) is for the purpose of communicating to our marketing lists via the use of MailChimp, a US-based operation. MailChimp is certified as compliant with current cross-border transfer regulation, including the EU-U.S. Privacy Shield Framework. Although other agencies may be used on occasion in the submission of our communications, no personal data is otherwise passed outside the UK. We do not transfer any of our personnel or HR data outside the UK.

We transfer the data we process on behalf of our clients outside the UK or EU inm the following circumstances: (a) if our client is based outside the UK or EU there will be an exchange of data with them when we submit to them tracking and other communications, (b) if our client designates courier despatch to a location outside the UK or EU, a transfer of some personal data may be required to the recipient country, specific only to details relating to that dispatch, (c) we may on occasion use a supporting Customer Services company outside the UK or EU processing data relevant only to a specific query, (d) the address parts of an address, although not the contact details included, may be passed to an address-checking processor with some storage outside the UK or EU during Customer Services operations.

A Data Protection Impact Assessment will be conducted before approval of any new procedure relating to the clouds or servers (or virtual servers) used to store or process data.

Contact Information

James Rhodes, Data Protection Officer, dataprotection@parcelhub.co.uk

Parcelhub Limited, Unit 6, Road No.2, Colwick Quays Business Park, Nottingham, NG4 2JY, United Kingdom

This policy was revised 13th June 2024