

## 1 The Controller - Who we are

- 1.1 Ballyvesey Holdings Limited. See section 15 for a list of individual Trading Companies.

## 2 Data Protection

- 2.1 Data Protection in the Ballyvesey Business Units administered by the Data Protection Committee (DPC).

- James Darragh (BVH Board Member & Legal Advisor)
- Gordon Willis (Head of Security & Governance)
- David Andrews (Data Protection Policy & Legislation)
- Darren Ward (Head of IT)

- 2.2 All members of the DPC have received training on data protection, Cyber Security and information security relating specifically to their responsibilities. In addition, at least one of the members of the DPC, will hold, or be working towards a General Data Protection Regulations Practitioner Certificate and at least one will hold, or be working towards a Certified Information Security Manager (CISM) Certificate.

- 2.3 The DPC can be contacted by emailing [dataprotection@ballyvesey.com](mailto:dataprotection@ballyvesey.com) or by writing to:

Data Protection  
Ballyvesey Holdings Limited  
607 Antrim Road  
Mallusk  
Newtownabbey  
BT36 4RF

## 3 Lawfulness and Compliance

- 3.1 Ballyvesey Holdings Limited undertakes to protect the rights and freedoms of all individuals whose data we process. We will only process where we have a legal basis to do so under Article 6 and uphold the principles in Article 5 of the General Data Protection Regulations (EU 2016/679), the General Data Protection Regulations (UK 2020), The Data Protection Act (UK 2018), and when applicable, the rights provided under statute by other any Act of Parliament having gained Royal Assent and any Amendment Acts or future Acts thereof. We accept the role of any competent authority, when recognised by UK government, where they have relevance in these matters.

- 3.2 We acknowledge that the only law repealed by the Data Protection Act (UK) 2018 is the Data Protection Act (UK) 1998 and that any other law introduced, or not repealed alongside this Act must also be recognised with equal authority, insofar as it has not been read down by any court of law to provide protection of the rights and freedoms of individuals protected by the Act.

## 4 How we gather personal data

4.1 Throughout the Group information is gathered in the normal course of business. The information we collect may include Public Data, Company Data, Third Party Data and Personal Data. Personal Data is protected in law by the General Data Protection Regulations EC 2016/679 and the Data Protection Act (UK) 2018. Where personal data is collected or provided to us a relevant privacy notice will be available summarising the following:

- who we are.
- who deals with our data protection.
- our purposes and legal basis for processing the personal data.
- our legitimate business interests in processing the personal data.
- who we may provide the personal data to
- whether we transfer the personal data to another member state, or international country.
- the length of time we will keep the personal data.
- a summary of your rights and freedoms to the processing of your personal data
- what may happen if you fail to provide / withdraw / object to the processing of the personal data, whether or not we process any personal data by automated means, including profiling individuals, or the existence of any monitoring of individuals.

4.2 Sources of personal data can come from individuals themselves, be provided to us by a third party where individuals themselves have previously agreed the legitimate interest to do so, be obtained from public records, or a competent authority.

## 5 Why we need personal data

5.1 Most often personal data will be needed along with other information to allow the group to operate according to its legitimate business interests. Other times we are required to process personal data to comply with a legal obligation, or to fulfil the requirements of a legally binding contract already in place, or that we may intend to enter into. Our business model has no intended processing in the public interest, unless a situation may occur which would morally require us to do so, for example to comply with the Whistle Blowing Policy, or the Modern Day Slavery Act. In an individual's vital interests, we may make a disclosure in an emergency where we believe they may be in threat of life or serious harm. Where processing is based on consent, we will obtain that consent and keep a record of doing so; individuals will have the right to withdraw their consent at any time, but this will not affect the legal standing of the processing that occurred prior to exercising this right.

## 6 Fairness and Transparency

- 6.1 We will process personal data fairly and with transparency to the individual who owns the personal data. We acknowledge the right of an individual to submit a Subject Access Request for any personal data which we hold about them. We will advise individuals if we transfer their personal data to a previously un-notified organisation to process in the business interests. We will notify any affected individuals of a breach if we have suffered a theft, destruction or other loss of their personal data as soon as the facts are fully known and cooperate with ICO, whilst complying with the Regulation.

## 7 Purpose Limitation

- 7.1 We will process personal data for the purposes which we have stated. If we need to process personal data for a new lawful purpose, we will be transparent and fair about this process.

## 8 Data Minimisation:

- 8.1 We will restrict collection of personal data to that which we really need. We will not ask for any information which is unnecessary. Once personal data is no longer necessary, we will responsibly destroy it, or return it to the individual who owns it. Where retention of data is required without the need to retain the personal data alongside it, we will use personal data anonymization and pseudonymisation to remove or disguise the personal element of the data.

## 9 Accuracy

- 9.1 We will take every reasonable step possible in the good practice of due diligence to ensure the accuracy of any personal data which we hold or process. Compliance checks, system auditing and staff training are conducted in order to minimise the risk and / or impact of inaccuracy in data generally. Where the personal data we hold is found to be incorrect an individual owning the personal data can request that we correct, rectify, erase or withhold it.

## 10 Storage Limitations:

- 10.1 Personal data will only be retained for as long as it is necessary and where we have a legitimate business purpose, or a legal obligation to do so. If we are found to hold personal data unjustifiably the individual who owns the personal data can ask us to return, erase, or destroy it. A retention policy forms part of any privacy notice available when personal data is collected.

## 11 Integrity and Confidentiality:

- 11.1 We will store and process personal data with appropriate security and protect it from unauthorised or unlawful processing, accidental loss, destruction, or damage, as far as we possibly can, using appropriate technical measures, monitoring and principles of least privilege.

- 11.2 We train our employees in various levels of data protection and information security protocols appropriate to their job roles. The group use robust usage policies as part of the terms and conditions of employment and use investigative and disciplinary procedures to enforce compliance with these policies throughout all levels of the workforce. Background checks and references are sought from new employees, in addition to a requirement for them to prove their identity. We try and obtain a copy of a passport of new employees to prove their identity, or otherwise another document to ensure their right to work within the UK and reduce the risk of modern slavery by requiring the employee to be in possession of their own passport in a safe environment. Records will be kept of identity documents, references and qualifications to demonstrate compliance with the regulation.
- 11.3 Employees are required to practice a clear desk policy and lock screens when away from their computer. Relevant technical controls and login permission groups are used to restrict access to relevant areas of software and data. Password complexity is enforced along with a significant minimum password length as is Multi Factory Authentication. Employees' requirements to remotely access systems with a work laptop from home or another location are subject to risk assessment based on needs, training and risks. If granted, remote access is through a Virtual Private Network (VPN) encrypted end to end using 256-bit technology. Employee permissions are reviewed and adjusted if changing roles, restricted or revoked if abused and removed completely when an employee leaves the group.
- 11.4 Electronic systems throughout the Group either use our own servers located in our premises, are hosted in Microsoft Azure or hosted by the system provider. Backups of all systems are frequently taken. At least one Member of the DPC has direct authority over our IT systems. Electronic Systems are supported by our internal team of professionals in the centralised ICT function which forms an integral part of the Group.
- 11.5 In addition to physical security present at hosting locations, access to our own premises is controlled by coded doors and / or swipe systems including biometrics at selected points. All server rooms are secured with appropriate locking mechanisms. Systems are protected by firewall protection, end point protection including anti-malware systems and access control systems. Incoming and outgoing mail is monitored and filtered, access to USB ports restricted, redundant hardware including drives are stored securely until dismantled and destroyed.
- 11.6 Portable devices such as laptops, tablets and smartphones are encrypted, secured by mobile device management systems which enforces pins and or passwords and anti-loss technology.
- 11.7 Physical files containing personal data are kept in locked areas, in fire resistant cabinets with restricted access. Any confidential waste records containing personal data are placed in locked letterbox bins until they can be shredded. Shredding is regularly conducted on site by a security cleared contractor under strict conditions.
- 11.8 The use of a Third-Party Network Access Agreement ensures adequate compliance inline with our own secure practices.

## 12 Controllers and Processors

- 12.1 Any Business Unit within the Group processing personal data at the point of contact is a “Data Controller.”
- 12.2 Any Business Unit within the Group sharing personal data, or accessing shared personal data within the group is a “Controller in Common.”
- 12.3 Any Business Unit within the Group processing personal data on behalf of another Business Unit within the group is a “Data Processor.”
- 12.4 Any party processing personal data on behalf of any Business Unit within the group, if in itself it is not part of the group, then they are a “Third Party Processor.”
- 12.5 Where a third-party processor is used, individuals to whom the personal data belongs will be informed that their information has been provided to the third party. If this action is underpinned by a legal obligation or a legitimate business interest, then consent is not required, providing that adequate safeguards are in place to ensure the processors meet the required compliance of the GDPR. As part of the adequate safeguards, the group requires all third-party processors to enter a legally binding contract to ensure compliance with GDPR and protection of the rights and freedoms of the individuals, to whom the original personal data belongs. Any Controller – Processor contract is in addition to any other Service Level Agreement in place (SLA).

## 13 Review Policy:

- 13.1 The DPC meets at regular intervals of every other month, or more often if needed. Any current business is dealt with at that time. Reviews of policies and procedures are part of the normal business of the DPC’s activities and they continue to make improvements as required to maintain compliance with all regular laws.

## 14 Rights and Freedoms:

- 14.1 Individuals have the right of subject access to (Article 15), and to be provided with a copy of, any personal data we hold. This request can be made using contact information provided at point 2 above. It must provide enough information to identify the data subject and satisfy the Controller of the applicant’s identity. Sufficient information to the specific nature of the request, and if known, the location of the information, should be made clear in the content to avoid any unnecessary, disproportionate effort in providing the personal data. We will then be required to respond within one month. Where the request is deemed complex, or requiring a disproportionate effort, we may then contact the individual to request that they reduce the focus, or scope of the their request, to only that which is needed, and / or to extend the period we are allowed to respond up to a further 2 calendar months.
- 14.2 If the subject believes that the personal data we hold is incorrect, they can ask us to rectify it (Article 16). Proof may be required to enable us to do this, otherwise a note may only be added to state that the information is in dispute.

- 14.3 If the subject believes that we should not have the personal data, because it is unnecessary, beyond the agreed retention period, or that the data has been unlawfully processed or obtained, then they can ask us to erase or return the personal data (Article 17).
- 14.4 Where any personal data is processed based on the reliance of consent and no other legitimate purpose can be justified, then the subject can withdraw their consent for any future use of the personal data (Article 18).
- 14.5 If an individual is unhappy about the way the Data Protection Committee deal with their rights and freedoms, they can complain in writing to:
- Chief Executive Officer  
Ballyvesey Holdings Limited  
607 Antrim Road  
Mallusk  
Newtownabbey  
BT36 4RF
- 14.6 The Chief Executive Officer or his nominated deputy will conduct an investigation and review of the circumstances and advise them of the findings along with any recommended actions within one month.
- 14.7 If the individual is still unsatisfied with the response of the Chief Executive Officer, or in fact at any other prior stage of the process, they can submit a report to the Information Commissioner's Office.

## 15 Trading Companies

Ballyvesey Industries Limited  
Ballyvesey Properties Limited  
Ballycraigy UK Properties Limited  
Montgomery Developments Limited  
Montgomery Transport (Ireland) Limited  
Montgomery Freight Management Limited  
MTG Customs Limited  
Sleator Plant Limited  
Norwest Plant Limited

Construction Equipment Distribution Limited  
t/a TDL Equipment  
DGC Limited  
Centurion Truck Rental Limited  
Sapphire Vehicle Solutions Limited  
Montracon Limited  
Midlands Truck & Van Limited  
Intercounty Truck & Van Limited  
West Pennine Trucks Limited

Ballyvesey Holdings Limited  
Ballycraigy Properties Limited  
Mallusk Business Park Limited  
Montgomery Transport Limited  
Montgomery Distribution Limited  
Montgomery Tank Services Limited  
Major Freight Limited  
Sleator Plant & Machinery (Ireland) Limited  
Eurofleet Rental Limited t/a Contract Plant  
Rental  
Genesis Equipment Sales Limited

DMC Trailers Limited  
Falcon Vehicle Solutions Limited  
Rockmount Vehicle Maintenance Limited  
Commercial Vehicle Auctions Limited  
Midlands Warehousing Limited  
Heathrow Truck Centre Limited

---

# Group Privacy Policy Statement

## Document Control

Reference: DOC ISMS 0023

Issue No: 1.0

Issue Date: 20/03/2024

Page: 7 of 7

---

## Document Control

The Data Protection Committee is the document owner and responsible for ensuring this policy remains current and up to date.

A current version of this document is available to all members of staff on the [Security and Governance SharePoint site](#) and is published by the Security and Governance function.

This policy was approved by the Data Protection Committee and is issued on a version controlled basis.

Representative of the DPC signature:



Date: 20/03/2024

## Change History Record

Issue	Description of Change	Date of Change
1.0	Initial Issue	
2.0	Review	20/03/2024