DATA PROTECTION POLICY

Contents

coolcare
admin made easy

T +44 (0) 113 385 3853
W coolcare.co.uk
E info@coolcare.co.uk

1. Policy statement

1.1. This policy applies to all LNT group companies including;

1.1.1. LNT Group Limited registered in England and Wales with company number 04929823 and whose registered office is Helios 47 1 Isabella Road, Garforth, Leeds, West Yorkshire, United Kingdom, LS25 2DY; and

1.1.2. Ideal Carehomes Limited registered in England and Wales with company number 10531219 and whose registered office is Helios 47 Isabella Road, Garforth, Leeds, United Kingdom, LS25 2DY; and

1.1.3. Ideal Carehomes (Number one) Limited registered in England and Wales with company number 7535382 and whose registered office is Helios 47 1 Isabella Road, Garforth, Leeds, West Yorkshire, United Kingdom, LS25 2DY; and

1.1.4. LNT Construction Limited registered in England and Wales with company number 2987352 and whose registered office is Helios 47 Isabella Road, Garforth, Leeds, United Kingdom, LS25 2DY; and

1.1.5. LNT Care Developments Limited registered in England and Wales with company number 09091938 and whose registered office is Helios 47 Isabella Road, Garforth, Leeds, United Kingdom, LS25 2DY; and

1.1.6. LNT Automotive Limited registered in England and Wales with company number 4598337 and whose registered office is Helios 47 Isabella Road, Garforth, Leeds, United Kingdom, LS25 2DY; and

1.1.7. Ginetta Cars Limited registered in England and Wales with company number 2744760 and whose registered office is Helios 47 Isabella Road, Garforth, Leeds, United Kingdom, LS25 2DY; and

1.1.8. CoolCare Limited registered in England and Wales with company number 3462441 and whose registered office is Helios 47 Isabella Road, Garforth, Leeds, United Kingdom, LS25 2DY; and

1.1.9. LNT Chemicals Limited registered in England and Wales with company number 7123117 and whose registered office is Helios 47 Isabella Road, Garforth, Leeds, United Kingdom, LS25 2DY; and

1.1.10. LNT Solutions Limited registered in England and Wales with company number 7166878 and whose registered office is Helios 47 Isabella Road, Garforth, Leeds, United Kingdom, LS25 2DY; and

1.1.11. LNT Aviation Limited registered in England and Wales with company number 7166878 and whose registered office is Helios 47 Isabella Road, Garforth, Leeds, United Kingdom, LS25 2DY; and

1.2. Collectively referred to in this policy as “LNT Group”/“us”/“we”/”our”.

1.3. Everyone has rights with regard to the way in which their personal data in handled. During the course of our activities we will collect, store and process personal data about our customers, suppliers and other third parties, and we recognise that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.

1.4. Data users, including all staff and third parties processing data on behalf of LNT Group (as defined above), are obliged to comply with this policy when processing personal data on our behalf. We take compliance with this policy very seriously. Any failure to comply puts both you and LNT Group at risk.

2. About this policy

2.1. The types of personal data that LNT Group may be required to handle includes information about current, past and prospective customers, business contacts, employees, staff, contractors, other individuals and others that we communicate with. The personal data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Data Protection Act 1998, and in substitution from 25 May 2018, the General Data Protection Regulation ((EU) 2016/679) (together the “Data Protection Legislation”) and other regulations.

2.2. This policy and any other documents referred to in it set out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.

2.3. This policy does not form part of any employee's contract of employment and may be amended at any time. We do, however, require all staff to comply with it.

2.4. This policy sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data.

2.5. LNT Group has nominated a Data Protection officer contactable at dataprotection@lntgroup.co.uk who is responsible for ensuring compliance with the Data Protection Legislation and with this policy. That post is currently held by Jonathan Wharam. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to your line manager and the privacy officer. The privacy officer is responsible for:

2.5.1. keeping the organisation updated about data protection responsibilities, risks and issues;

2.5.2. reviewing data protection procedures and policies on a regular basis;

2.5.3. arranging data protection training and advice for staff members;

2.5.4. answering questions on data protection from other members of the organisation;

2.5.5. responding to individuals such as clients and employees who wish to know which data is being held on them by us; and

2.5.6. checking and approving with third parties that handle the company's data any contracts or agreement regarding data processing.

3. Definition of data protection terms

3.1. Data is information which is stored electronically, on a computer, or in certain paper-based filing systems;
3.2. Data subjects means all living individuals about whom we hold Personal Data;
3.3. Personal data means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour;
3.4. Data controllers are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with the Data Protection Legislation. We are the data controller of all personal data used in our business for our own commercial purposes;
3.5. Data users are those of our employees whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times;
3.6. Data processors include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on LNT Group' behalf;
3.7. Processing is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties;
3.8. Sensitive personal data, or special categories of data include information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data and special categories of data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned; and
3.9. Supervisory Authority means the Information Commissioner's Office or other relevant supervisory authority.

4. Data protection principles

4.1. Anyone processing personal data must comply with the following principles of good practice. These provide that personal data must be:
4.1.1. processed fairly, lawfully and in a transparent manner;
4.1.2. processed for specified, explicit and legitimate purposes and in an appropriate way;
4.1.3. adequate, relevant and limited to what is necessary for the purpose;
4.1.4. accurate and kept up to date;
4.1.5. not kept longer than necessary for the purpose; and
4.1.6. processed in line with data subjects' rights including in respect of the security of personal data.

5. Fair and lawful processing

5.1. The Data Protection Legislation is not intended to prevent the processing of personal data, but to ensure that it is done fairly and lawfully in accordance with the rights of the data subjects.
5.2. For personal data to be processed lawfully, they must be processed on the basis of one of the legal grounds set out in the Data Protection Legislation. These include, among other things, the data subject's consent to the processing, or that the processing is necessary for the performance of a contract with the data subject, for the compliance with a legal obligation to which the data controller is subject, or for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data, or special categories of data are being processed, additional conditions must be met. When processing personal data as data controllers in the course of our business, we will ensure that those requirements are met and ensure that all staff who are responsible for processing personal data will be aware of the conditions for processing. It is important that you comply with this policy at all times and notify your line manager or the privacy officer if you have any queries. Consent to processing can be revoked at any time.

6. Consent

6.1. A data subject consents to processing of their personal data if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked

coolcare
admin made easy
T +44 (0) 113 385 3853
W coolcare.co.uk
E info@coolcare.co.uk

boxes or inactivity are unlikely to be sufficient. If consent is given in a document which deals with other matters, then the consent must be kept separate from those other matters.

6.2. Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to process personal data for a different and incompatible purpose which was not disclosed when the data Subject first consented.

6.3. Unless we can rely on another legal basis of processing, explicit consent is usually required for processing sensitive personal data, and for cross border data transfers. Usually we will be relying on another legal basis (and not require explicit consent) to process most types of sensitive data. Where explicit consent is required, you must issue a fair processing notice to the data subject to capture explicit consent.

6.4. You will need to evidence consent captured and keep records of all Consents so that we can demonstrate compliance with Consent requirements.

7. Processing for limited purposes

7.1. In the course of our business, we may collect and process personal data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, business partners, sub-contractors in technical, payment and delivery services, credit reference agencies and others).

7.2. We will only process personal data for the specific purposes for which we have obtained consent or otherwise have a basis for processing in accordance with the Data Protection Legislation. We will notify those purposes to the data subject when we first collect the data or as soon as possible thereafter.

8. Notifying data subjects

8.1. If we collect personal data directly from data subjects, we will inform them about:

8.1.1. who is collecting the personal data and how it is being collected;

8.1.2. the purposes for which we intend to process that personal data;

8.1.3. the types of third parties, if any, with which we will share or to which we will disclose that personal data;

8.1.4. identity and contact details of any data controllers;

8.1.5. details of transfers to other countries and safeguards;

8.1.6. the retention period; and

8.1.7. the means with which data subjects can limit our use and disclosure of their personal data, and any other rights they have in respect of the data.

8.2. If we receive personal data about a data subject from other sources, we will provide the data subject with this information as soon as possible thereafter.

8.3. We will also inform data subjects whose personal data we process that we are the data controller with regard to that data, and who the privacy officer is.

9. Adequate, relevant and non-excessive processing

9.1. We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject.

9.2. We will keep full and accurate records of all our data processing activities, including records of data subjects' consents and procedures for obtaining consents.

10. Accurate data

10.1. We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

10.2. Individuals may ask that we correct inaccurate personal data that we hold relating to them. If you believe that any data we hold is inaccurate, you should notify your line manager and the privacy officer.

11. Timely processing

11.1. We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. We will maintain a retention policy and procedure and take all reasonable steps to ensure that we destroy, or erase from our systems, all data which is no longer required.

coolcare
admin made easy

T +44 (0) 113 385 3853
W coolcare.co.uk
E info@coolcare.co.uk

12. Processing in line with data subject's rights

12.1. We will process all personal data in line with data subjects' rights, in particular their right to:
- 12.1.1. request access to any data held about them by a data controller (see also clause 17);
- 12.1.2. prevent the processing of their data for marketing purposes;
- 12.1.3. ask to have inaccurate data amended (see also clause 10);
- 12.1.4. request a copy of their data in a structured format (see also clause 18); and
- 12.1.5. request that information held on them is deleted or removed (see also clause 19.

13. Data security

13.1. We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. We will regularly evaluate the effectiveness of these measures to ensure security of our processing pf personal data. You must exercise particular care in protecting sensitive personal data from loss and unauthorised access, use or disclosure.

13.2. We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if it agrees to comply with those procedures and policies, or if it puts in place adequate measures itself.

13.3. We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:
- 13.3.1. confidentiality means that only people who are authorised to use the data can access it;
- 13.3.2. integrity means that personal data should be accurate and suitable for the purpose for which it is processed; and
- 13.3.3. availability means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on our central computer system instead of individual PCs.

13.4. Security procedures include:
- 13.4.1. entry controls. Any stranger seen in entry-controlled areas should be reported;
- 13.4.2. secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold confidential information of any kind (personal information is always considered confidential);
- 13.4.3. methods of disposal. Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required; and
- 13.4.4. equipment. Data users must ensure that individual monitors do not show confidential information to passers-by and that they lock/log off from their computer/mobile phone when it is left unattended.
- 13.4.5. Devices. All PCs, Laptops and Mobiles must be password protected.

14. Transferring personal data to a country outside the EEA

14.1. We may transfer any personal data we hold to a country outside the European Economic Area ("EEA") only after discussing it further with the privacy officer and provided that one of the following conditions applies:
- 14.1.1. the country to which the personal data is transferred ensures an adequate level of protection for the data subjects' rights and freedoms on the basis of either a finding of adequacy by the EU Commission or other appropriate safeguards provided for in the Data Protection Legislation;
- 14.1.2. the data subject has given his consent; or
- 14.1.3. the transfer is required by law.

14.2. Subject to the requirements in clause 14.1 above, personal data we hold may also be processed by staff operating outside the EEA who work for us or for one of our suppliers. These staff may be engaged in, among other things, the fulfilment of contracts with the data subject, the processing of payment details and the provision of support services.

15. Data Protection Impact Assessment (DPIA)

15.1. We will implement appropriate technical and organisational measures to ensure compliance with data privacy principles taking into consideration the nature, scope, context and purposes of processing and the risks of varying likelihood and severity for the rights and freedoms of data subjects posed by the processing.

15.2. We will conduct DPIAs in respect to high risk processing. DPIAs should be carried out and discussed with the privacy officer when implementing major system or business change programs involving the processing of personal data including:

coolcare
admin made easy
T +44 (0) 113 385 3853
W coolcare.co.uk
E info@coolcare.co.uk

15.2.1. use of new or changing technologies (programs, systems or processes);
15.2.2. large scale processing of sensitive personal data; and
15.2.3. large scale, systematic monitoring of a publicly accessible area.

15.3. The DPIA must include:
15.3.1. a description of the processing, its purposes and the legitimate interests if appropriate;
15.3.2. an assessment of the necessity and proportionality of the processing in relation to its purpose;
15.3.3. an assessment of the risk to individuals; and
15.3.4. the risk mitigation measures in place and demonstration of compliance.

16. Disclosure and sharing of personal information

16.1. We may share personal data we hold with any member of our group, which means our subsidiaries, our ultimate holding company and its subsidiaries, as defined in section 1159 of the UK Companies Act 2006.

16.2. You may only share personal data we hold with another employee, agent or representative of LNT Group if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

16.3. We may also disclose personal data we hold to third parties:
16.3.1. if sharing the personal data complies with our privacy policy and, if required, the data subject's consent has been obtained;
16.3.2. the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
16.3.3. we have a written contract in place with the third party which contains GDPR approved third party clauses;
16.3.4. if we sell or buy any business or assets, in which case we may disclose personal data we hold to the prospective seller or buyer of such business or assets; or
16.3.5. if we or substantially all of our assets are acquired by a third party, in which case personal data we hold will be one of the transferred assets; or
16.3.6. if we are under a duty to disclose or share a data subject's personal data in order to comply with any legal obligation, or in order to enforce or apply any contract with the data subject or other agreements; or
16.3.7. to protect our rights, property, or safety of our employees, customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

17. Dealing with subject access requests

17.1. Data subjects may make a formal request for information we hold about them free of charge. This should be made in writing addressed to the privacy officer although a data subject is entitled to make the request to any member of staff. The request may be made in writing by any means, including email, fax or via a web enquiry. Employees who receive a written request or think they may have received a request should forward it to their line manager and privacy officer immediately.

17.2. When receiving telephone enquiries, we will only disclose personal data we hold on our systems if the following conditions are met:
17.2.1. we will check the caller's identity to make sure that information is only given to a person who is entitled to it; and
17.2.2. we will suggest that the caller put their request in writing if we are not sure about the caller's identity and where their identity cannot be checked.

17.3. Subject to the provision of limited information in accordance with clause 17.2 above, employees should not respond to a subject access request without first discussing the request with their line manager/the privacy officer. Please note that there are strict requirements placed on all organisations in respect of dealing with and responding to subject access requests. Any failure of LNT Group in this respect could result in significant fines and other penalties being imposed on LNT Group. It is therefore important that you immediately notify your line manager and the privacy officer of any subject access request.

18. Data portability

18.1. Data subjects have the right to receive a copy of their data in a structured format and for their data to be transferred directly to another system, free of charge. Any such request should be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals. If you need further information, please contact your line manager or the privacy officer.

19. Right to be forgotten

19.1. Data subjects have the right to request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with such request. This type of request can only be refused if an exemption applies. The privacy officer will make the final decision.

20. Requests made by a data subject in respect of their rights

20.1. Any requests made by a data subject in relation to any of the rights which they have in relation to their personal data should be referred to the privacy officer as soon as possible to ensure that such requests are dealt with in a timely and appropriate manner.

21. Reporting breaches

21.1. All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

21.1.1. investigate the failure and take remedial steps if necessary;

21.1.2. maintain a register of compliance failures; and

21.1.3. notify the Supervisory Authority of any compliance failures that are material either in their own right or as part of a pattern of failures.

21.2. Please report any failures to your line manager and the privacy officer. Please note that there are strict requirements placed on all organisations in respect of reporting a breach to the Supervisory Authority. Any failure of LNT Group in this respect could result in significant fines and other penalties being imposed on LNT Group. It is therefore important that you immediately notify your line manager and the privacy officer of any breach or suspected breach.

22. Monitoring

22.1. Everyone must observe this policy. The privacy officer has overall responsibility for this policy. They will monitor compliance regularly to make sure the policy is being adhered to.

23. Changes to this policy

23.1. We reserve the right to supplement or amend this policy at any time. Where appropriate, we will notify data subjects of those changes by mail or email. Any new or modified policy will be circulated to staff.

24. Contact/Information

24.1. If you have any queries or require any further assistance or information in relation to any of the contents of this policy, please contact Jonathan Wharam – Data Protection Officer at dataprotection@lntgroup.co.uk.

Date reviewed: 13.12.19
Reviewer: Fiona Hale, Managing Director

Date	Created/Reviewed By	Comments/Updates Made
12.19	Fiona Hale	Reviewed, no updates made.
04.22	Fiona Hale	Updated DPO to Jonathan Wharam