[GDPR] General Data Protection Policy Statement

Contents

1. Policy Summary

1.1. The Senior Management Team within Tracgroup , are [within the context of its Information Security Policy) committed to comply with all relevant UK and EU laws in respect to data privacy, and towards the protection of the "rights and freedoms" of individuals whose information Tracgroup, as data controller collect. Most notably in accordance with the General Data Protection Regulation (GDPR), which comes into force from May 2018. To that end, the Senior Management Team have developed, implemented, maintain and continuously improve a documented Personal Information Management System ('PIMS') across all [its] locations.

2. Scope

2.1. This policy aims to meet the requirements of the (GDPR) across all [its] locations, customers, employees, partners and affiliates of Tracgroup whom act as processor on behalf of [our] data subjects. Significant changes to data privacy laws in the EU/UK have led to Tracgroup reviewing its existing policies and procedures to ensure it meets the new criteria and to safeguard our business and its customers from the latest threats towards the overall rights and freedoms of individuals.

2.2. The General Data Protection Regulation replaces the EU Data Protection Directive of 1995 and supersedes the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC. Its purpose is to protect the "rights and freedoms" of living individuals, and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

2.3. Tracgroup is responsible for the on-going maintenance, effectiveness and ultimate alignment of this policy to fulfil our legal/regulatory requirements; and remains accountable to the board of directors on its overall performance.

3. Objectives of the PIMS (Personal Information Management System)

3.1. The objectives for the PIMS will enable Tracgroup to;

(a) meet its own privacy requirements as a data controller;

(b) to meet all necessary compliance obligations as per the GDPR;

(c) impose controls in line with Tracgroup's Risk Management strategy;

(d) ensure Tracgroup meet(s) all applicable statutory, regulatory, contractual and professional duties and;

(e) that it protects the interests of data subjects, third parties, affiliated data processors and other interested parties.

3.2. Tracgroup is committed towards the fulfilment of all its compliance requirements relating to Data Privacy and its subsequent practices including, but not limited to;

3.2.1. Processing personal information only where this is strictly necessary for legitimate business purposes;

3.2.2. Collecting only minimum personal information required for these purposes and not processing excessive personal information;

3.2.3. Providing clear information to individuals about how their personal information will be used and by whom;

3.2.4. Only processing relevant and adequate personal information;

3.2.5. Processing personal information fairly and lawfully;

3.2.6. Maintaining an inventory of the categories of personal information processed by Tracgroup as both data controller and processor.

3.2.7. Maintaining its accuracy and, where necessary, kept up to date;

3.2.8. Retaining personal information only for as long as is necessary for both legal and/or regulatory reasons or, for other legitimate purposes – expressly agreed;

3.2.9. Respecting an individuals' rights in relation to their personal information, including their right to access;

3.2.10. Maintaining its security and accessibility;

3.2.11. Only transferring personal information outside the EU in circumstances where it can be adequately protected and is necessary.

3.2.12. The application of the various exemptions allowable by the current data protection legislation;

3.2.13. Developing and implementing a PIMS to enable the policy to be implemented effectively;

3.2.14. Where appropriate, identifying both internal and external stakeholders and the degree to which these stakeholders are involved in the governance of Tracgroup PIMS; and

3.2.15. The identification of stakeholders with specific responsibility and accountability for the PIMS.

4. Notification

4.1. Tracgroup has notified the Information Commissioner that it is a data controller and that it processes certain information about data subjects. Tracgroup have identified all personal data assets that it processes and is contained within the Data Inventory Register.

4.2. A copy of the ICO notification details are retained by Tracgroup.

4.3. The ICO notification is renewed annually each year.

4.4. Tracgroup is responsible, each year, for reviewing the details of notification, in the light of any changes to Tracgroup's activities (as determined by changes to the Data Inventory Register and the management review) and to any additional requirements identified by means of data protection impact assessments.

4.5. The policy applies to all Employees/Staff [and its interested parties] of Tracgroup such as outsourced suppliers. Any breach towards the GDPR or this PIMS will be dealt with under Tracgroup's disciplinary policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

4.6. Partners and any third parties working with or for Tracgroup, and who have or may have access to personal information, will be expected to have read, understood and to comply with this policy. No third party may access personal data held by Tracgroup without having first provided a GDPR Policy, which imposes on the third-party obligations no less onerous than those to which Tracgroup is committed, and which gives Tracgroup the right to audit compliance with the agreement.

5. Definitions

5.1. Territorial scope – the GDPR will apply to all controllers that are established in the EU (European Union) who process the personal data of data subjects, in the context of that establishment. It will also apply to controllers outside of the EU that process personal data to offer goods and services, or monitor the behaviour to data subjects who are resident in the EU.

5.2. Establishment – the main establishment of the controller in the EU will be the place in which the controller makes the main decisions as to the purpose of its data processing activities. The main establishment of a processor in the EU will be its administrative centre. If a controller is based outside the EU, it will have to appoint a representative in the jurisdiction in which the controller operates, to act on behalf of the controller and deal with supervisory authorities.

5.3. Personal data – any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

5.4. Special categories of personal data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

5.5. Data controller – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

5.6. Data subject – any living individual who is the subject of personal data held by Tracgroup.

5.7. Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

5.8. Profiling – is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse, or predict that person’s performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

5.9. Personal data breach – a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the controller to report personal data breaches (within 72 hours) to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

5.10. Data subject consent - means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

5.11. Child – the GDPR defines a child as anyone under the age of 16 years old. The processing of personal data of a child under 13 years of age is only lawful if parental or custodian consent has been obtained.

5.12. Third party – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

5.13. Filing system – any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

6. Responsibilities

6.1. Tracgroup is a data controller and data processor under the GDPR.

6.2. Senior Management and all those in managerial or supervisory roles throughout Tracgroup are responsible for developing and encouraging correct information handling practices; responsibilities of which are set out within individual job descriptions.

6.3. Tracgroup Board of Directors directly responsible for the management of personal information within Tracgroup and for ensuring overall compliance with data protection legislation and best practice can be demonstrated. These accountabilities include;

6.3.1. The development and implementation of the PIMS as required by this policy; and

6.3.2. The security and risk management in relation to compliance with the policy.

6.4. Tracgroup Board of Directors considered to be suitably qualified and experienced, have been appointed to take overall responsibility for Tracgroup's compliance with this policy and the day-to-day management on this basis and, in particular, has direct responsibility for ensuring that Tracgroup complies with the GDPR, as do the senior management team in respect to the data processing activities that takes place within their area of responsibility.

6.5. Tracgroup has specific responsibilities in respect of procedures such as the 'Access Request', and is the first point of call for Employees/Staff seeking clarification on any aspect of data protection compliance.

6.6. Compliance with data privacy legislation is the responsibility of all active employees of Tracgroup whom process personal information on behalf of the data controller.

6.7. Tracgroup's Training Policy sets out specific training and awareness requirements in relation to specific roles and to members of Tracgroup generally.

6.8. Members of Tracgroup are responsible for ensuring that any personal data supplied by them, and that is about them, to Tracgroup is accurate and up-to-date.

7. Risk Assessment

7.1. To ensure that Tracgroup are aware of any risks associated with the processing of the variable types of personal information [we] hold and process.

7.2. Tracgroup has a process for assessing the level of risk to individuals associated with the processing of their personal information. Assessments will also be carried out in relation to processing tasks undertaken by other organisations on behalf of Tracgroup. Tracgroup shall manage any risks which are identified by the risk assessment to reduce the likelihood of a nonconformance with this policy.

7.3. Where a type of processing, uses new technologies and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the "rights and freedoms"

of natural persons, Tracgroup shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

7.4. A single assessment may address a set of similar processing operations that present similar high risks.

7.5. Where, as a result of a Privacy Impact Assessment, it is clear that Tracgroup is about to commence processing of personal information that could cause damage and/or distress to the data subjects, the decision as to whether or not Tracgroup may proceed must be escalated for review. Tracgroup shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, escalate the matter to the Information Commissioners Office [supervisory authority].

7.6. Appropriate controls will be selected, typically relating to cyber security, and applied to reduce the level of risk associated with processing individual data to an acceptable level, by reference to Tracgroup's documented risk acceptance criteria and the requirements of the GDPR.

8. Data protection principles

8.1. All processing of personal data must be done in accordance with the following data protection principles and any/all supplementary Tracgroup policies and procedures determined to offer additional mitigation steps;

8.1.1. Personal data must be processed lawfully, fairly and transparently.

8.1.2. Tracgroup's Fair Processing Procedure is set out.

8.1.3. Demonstrate a transparent and easily accessible policies relating to the processing of personal data and the exercise of individuals' "rights and freedoms". Information must be communicated to the data subject in an intelligible form using clear and plain language.

8.1.4. The specific information that must be provided to the data subject must as a minimum include:

8.1.4.1. the identity and the contact details of the controller and, if any, of the controller's representative;

8.1.4.2. the contact details of the Data Protection Officer, where applicable;

8.1.4.3. the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

8.1.4.4. the period for which the personal data will be stored;

8.1.4.5. the existence of the rights to request access, rectification, erasure or to object to the processing;

8.1.4.6. the categories of personal data concerned;

8.1.4.7. the recipients or categories of recipients of the personal data, where applicable;

8.1.4.8. where applicable, that the controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data;

8.1.4.9. any further information necessary to guarantee fair processing.

8.1.5. Personal data can only be collected for specified, explicit and legitimate purposes.

8.1.6. Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the Information Commissioner as part of Tracgroup's GDPR registration.

8.1.7. Personal data must be adequate, relevant and limited to what is necessary for processing.

8.1.8. Tracgroup is responsible for ensuring that information, which is not strictly necessary for the purpose for which it is obtained, is not collected.

8.1.9. All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must be approved by Tracgroup.

8.1.10. Tracgroup will ensure that, on an [annual] basis all data collection methods are reviewed by [internal auditors] to ensure that collected data continues to be adequate, relevant and not excessive.

8.1.11. If data is given or obtained that is excessive or not specifically required by Tracgroup – as per the documented procedures, the appointed Data Protection Officer is responsible for ensuring that it is securely deleted or destroyed in line with internal policies.

8.1.12. Personal data must be accurate and kept up to date.

8.1.13. Data that is kept for a prolonged period of time must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.

8.1.14. Tracgroup is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.

8.1.15. It is also the responsibility of individuals to ensure that data held by Tracgroup is accurate and up-to-date.

8.2. Employees/customers should notify Tracgroup of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of Tracgroup to ensure that any notification regarding change of circumstances is noted and acted upon.

8.3. Tracgroup is responsible for ensuring that appropriate additional steps are taken to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.

8.4. On at least an annual basis, Tracgroup will review all the personal data maintained, by reference to the Data Inventory Register, and will identify any data that is no longer required in the context of the registered purpose and will arrange to have that data securely deleted/destroyed. Tracgroup reviews this information on an annual basis, and removes information that is 6 years or older in alignment with HMRC, unless regulation requires that information is to be retained for longer.

8.5. Tracgroup is responsible for making appropriate arrangements that, where third party organisations may have been passed inaccurate or out-of-date personal information, to correct or remove the information concerned.

9. Personal Data Format

9.1. Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.

9.2. Where personal data is retained beyond the processing date, it will be minimised/encrypted/pseudonymised/archived in order to protect the identity of the data subject in the event of a data breach.

9.3. Personal data will be retained in line with the retention of records procedure and, once its retention date is passed, it must be securely destroyed as set out in this procedure.

9.4. Tracgroup must specifically approve any data retention that exceeds the retention periods, and must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation. This approval must be written.

10. Data Processing

10.1. Personal data must be processed in a manner that ensures its security

10.2. Appropriate technical measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

10.3. These controls have been selected based on identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed.

10.4. Tracgroup's compliance with this principle is contained in its Cyber Security Management System.

10.5. Security controls will be subject to audit and review.

10.6. Personal data shall not be transferred to a country or territory outside the European Union [EU] unless that country or territory ensures an adequate level of protection for the 'rights and freedoms' of data subjects in relation to the processing of personal data.

10.7. The transfer of personal data outside of the EU is prohibited unless one or more of the specified safeguards or exceptions apply.

11. PCI DSS Compliance

11.1. In addition to the controls specified within the PIMS, Tracgroup remain compliant to all associated PCI DSS requirements, within the scope of its operational activities through its Internal Audit program, annual registration and external compliance assessments carried out by a certified PCI DSS partner.

12. Copyright/IP Rights

12.1. All rights, in the Tracgroup website, its customer Portals and its contents, are owned by or licensed to Tracgroup, or otherwise used by Tracgroup as permitted by applicable law. Copyright ownership of images are labelled alongside the image except for the header images, copyright ownership of these as detailed at the bottom of this page.

12.2. By accessing Tracgroup's webpages, it is under the agreement that access towards its contents are solely for private use, for any commercial and public use.

12.3. Except as permitted above, all rights and contents are available under the pretext that they're not to be copied, stored in any medium (including in any other website), distributed, transmitted, re-transmitted, broadcast, modified, or shown in, without the prior written permission of Tracgroup or in accordance with the Copyright, Designs and Patents Act 1988.

13. Safeguards

13.1. An assessment of the adequacy by the data controller of its safeguards are carried out, addressing the following factors;

13.1.1. the nature of the information being transferred;

13.1.2. the country or territory of the origin, and ultimate [final] destination, of the information;

13.1.3. how the information will be used and for how long;

14. Accountability

14.1. The GDPR introduces the principle of accountability which states that the controller is not only responsible for ensuring compliance but for demonstrating that each processing operation complies with the requirements of the GDPR.

14.2. Specifically, controllers are required to maintain necessary documentation of all processing operations, implement appropriate security measures, perform PIAs (Privacy Impact Assessment), comply with requirements for prior notifications, or approval from supervisory authorities and appoint a Data Protection Officer if required.

15. Data subjects' rights

15.1. Data subjects have the following rights regarding data processing, and the data that is recorded about them;

15.1.1. To make subject access requests regarding the nature of information held and to whom it has been disclosed.

15.1.2. To prevent processing likely to cause damage or distress.

15.1.3. To prevent processing for purposes of direct marketing.

15.1.4. To be informed about the mechanics of automated decision-taking process that will significantly affect them.

15.1.5. Not to have significant decisions that will affect them taken solely by automated process.

15.1.6. To sue for compensation if they suffer damage by any contravention of the GDPR.

15.1.7. To take action to rectify, block, erased, including the right to be forgotten, or destroy inaccurate data.

15.1.8. To request the ICO to assess whether any provision of the GDPR has been contravened.

15.1.9. The right for personal data to be provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.

15.1.10. The right to object to any automated profiling without consent.

15.2. Data subjects may make data access requests by completing an Access Request form, which can be requested via email to GDPR@tracgroup.co.uk, this procedure also describes how Tracgroup will ensure that its response to the data access request complies with the requirements of the Regulation.

16. Complaints

16.1. Data Subjects whom wish to complain to Tracgroup about how their personal information has been processed may lodge their complaint directly with the Complaints process at Tracgroup.

16.2. Data subjects may also complain directly to the Information Commissioners Office.

16.3. Where data subjects wish to complain about how their complaint has been handled, or appeal against any decision made following a complaint, they may lodge a further complaint to Tracgroup.

17. Consent

17.1. Tracgroup understands 'consent' to mean that it has been explicitly and freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she by statement, or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The consent of the data subject can be withdrawn at any time.

17.2. Tracgroup understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing.

17.3. In most instances consent to process personal and sensitive data is obtained routinely by Tracgroup using standard consent documents [reference] e.g. when a new member of staff signs a contract of employment, or during induction for participants on programmes.

17.4. Where Tracgroup provides online services to children, parental, or custodial authorisation must be obtained. This requirement applies to children under the age of 16.

18. Security of data

18.1. All Employees/Staff are responsible for ensuring that any personal data which Tracgroup holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by Tracgroup to receive that information and has entered into a confidentiality agreement.

18.2. All personal data should be accessible only to those who need to use it, and access may only be granted in line with the Access Control Procedure. You should form a judgment based upon the sensitivity and value of the information in question, but personal data must be kept:

18.2.1. in a lockable room with controlled access; and/or

18.2.2. in a locked drawer or filing cabinet; and/or

18.2.3. if computerised, password protected in line with corporate requirements in the Access Control Procedure, and/or

18.2.4. stored on (removable) computer media which are encrypted.

18.3. Care must be taken to ensure that PC screens and terminals are not visible except to authorised Employees of Tracgroup. All Employees are required to enter into an Acceptable Use Agreement before they are given access to Tracgroup's information of any sort.

18.4. Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit [written] authorisation. As soon as

manual records are no longer required for day-to-day client support, they must be removed to secure archiving.

18.5. Personal data may only be deleted or disposed of in line with the Data Retention Procedure. Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and immediately destroyed as required before disposal.

19. Rights of access to data

19.1. Data subjects have the right to access any personal data (i.e. data about them) which is held by Tracgroup in electronic format and manual records which form part of a relevant filing system. This includes the right to inspect confidential personal references received by Tracgroup, and information obtained from third-party organisations about that person.

19.2. Access Requests are dealt with as per the published 'Access Request' form, available through our Website, or upon request via telephone or email to GDPR@tracgroup.co.uk.

20. Disclosure of data

20.1. Tracgroup must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All Employees should exercise caution when asked to disclose personal data held on another individual to a third party [and will be required to attend specific training that enables them to deal effectively with any such risk]. It is important to bear in mind whether disclosure of the information is relevant to, and necessary for, the conduct of Tracgroup's business.

20.2. The GDPR permits certain disclosures without consent so long as the information is requested for one or more of the following purposes;

20.2.1. to safeguard national security;

20.2.2. prevention or detection of crime including the apprehension or prosecution of offenders;

20.2.3. assessment or collection of tax duty;

20.2.4. discharge of regulatory functions (includes health, safety and welfare of persons at work);

20.2.5. to prevent serious harm to a third party;

20.2.6. to protect the vital interests of the individual, this refers to life and death situations.

20.3. All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by Tracgroup.

21. Disposal of records

21.1. Personal data must be disposed of in a way that protects the "rights and freedoms" of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion) and in line with the secure disposal.

22. Data Protection Officer

22.1. For any/all enquiries relating to this policy or any data privacy practices carried out by Tracgroup, please contact a Director.