General Data Protection Regulation (GDPR) - Data Protection Policy Statement

TouchByte Ltd

22nd December 2021

Category	Data Protection
Version	3.0
Classification	Internal

Document Control

Organisation	TouchByte Ltd
Title	Data Protection Policy
Author	Mark Bailey
Filename	GDPR_V3.doc
Owner	Mark Bailey, Technical Director
Subject	Data Protection
Protective Marking	None
Review date	20th Dec 2021
Location	SharePoint: Documents -> Policies & Statements -> Data Protection

Revision History

Revision Date	**Version Number**	**Revised By**	**Description of Revision**
30/03/18	1.1	Nicola Oldale	Initial document
20/5/18	2.0	Mark Bailey	Various amendments
22/12/21	3.0	Graham Love	Annual review

Document Approvals

This document requires the following approvals:

Sponsor Approval	**Name**	**Date approved**
Managing Director	Jeremy Sneller	22/12/21

Document Distribution

This document will be distributed to:

Name	**Job Title**	**Email Address / Location**
Alison Hancock	Finance Director	alison.hancock@touchbyte.co.uk
Graham Love	Chief Operations Officer	graham.love@touchbyte.co.uk
Mark Bailey	Technical Director	Mark.bailey@touchbyte.co.uk
Jeremy Sneller	Managing Director	jeremy.sneller@touchbyte.co.uk
Harrison Hayward-Gore	Lead Software Engineer	harrison.hayward-gore@touchbyte.co.uk
Ellen O'Rourke	Head of Marketing	ellen.orourke@touchbyte.co.uk

Data Protection Policy Statement

1. Policy, scope and objectives

TouchByte Ltd is committed to compliance with all relevant UK and EU laws in respect of personal data, and to protecting the "rights and freedoms" of individuals whose information TouchByte collects in accordance with the General Data Protection Regulation (GDPR).

The General Data Protection Regulation 2016 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.

TouchByte is committed to complying with data protection legislation and good practice including:
a. processing personal information only where this is strictly necessary for legitimate organisational purposes;
b. collecting only the minimum personal information required for these purposes and not processing excessive personal information
c. providing clear information to individuals about how their personal information will be used and by whom;
d. only processing relevant and adequate personal information;
e. processing personal information fairly and lawfully;
f. maintaining an inventory of the categories of personal information processed by TouchByte;
g. keeping personal information accurate and, where necessary, up to date;
h. retaining personal information only for as long as is necessary for legal or regulatory reasons or, for legitimate organisational purposes;
i. respecting individuals' rights in relation to their personal information, including their right of subject access;
j. keeping all personal information secure;
k. only transferring personal information outside the EU in circumstances where it can be adequately protected;
l. the application of the various exemptions allowable by data protection legislation;
m. developing and implementing a documented personal information management system (PIMS) to enable the policy to be implemented;

1.1 Scope

1.1.1 The scope of the documented personal information management system (PIMS) takes into account all data used, captured, held and discarded by TouchByte, where this is under their control. It describes the processes and procedures for how and when the data is handled, stored and removed securely. It also describes how TouchByte communicate all mandatory practices both internally to their employees and partners, and to customers and other external relevant users.

1.1.2 The policy applies to all Employees [and interested parties] of TouchByte. Any breach of the GDPR or this PIMS will be dealt with under TouchByte'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.

1.1.3 Partners and any third parties working with or for TouchByte, 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 TouchByte without having first entered into a Data Confidentiality Agreement which imposes on the third-party obligations no less onerous than those to which TouchByte is committed, and which gives TouchByte the right to audit compliance with the agreement.

1.2 Objectives of the PIMS

The PIMS objectives are as follows:
1 Provide clear methodologies, guidelines and practices for TouchByte personnel with regard to the management and control of all data that flows in and out of TouchByte
2 Have in place clear objectives and obligations as applicable to all levels of employees (as the scope and control of external individuals or organisations is not under TouchByte's control or responsibility).
3 Illustrate levels of acceptable risk balanced with appropriate levels of control
4 Meet applicable statutory, regulatory, contractual and professional levels of control.
5 Establish appropriate methods of checks/audits/reviews to ensure that the information and
6 methodologies used are being followed, kept up-to-date and reviewed on a regular basis.

2. <u>ICO & Data Controller/Processor</u>

2.1 TouchByte is a data controller and data processor under the GDPR and has notified the Information Commissioner of this and that, as such, it processes certain information about data subjects. TouchByte has identified all the personal data that it processes and this is contained in the Data Inventory Register.

2.2 A copy of the ICO notification details is retained by Mark Bailey, the Data Protection Officer/GDPR Owner who also is responsible for maintaining a record of all ICO notifications as specified within the Data Breach Response Policy.

2.3 The ICO notification is renewed annually on 1st October annually.

2.4 The ICO registration reference is ZA139673.

3. Responsibilities under the General Data Protection Regulation

3.1 Overall, TouchByte's Senior Management are responsible for encouraging good information handling practices within the organisation. However, compliance with data protection legislation is the responsibility of all members of TouchByte who process personal information.

3.2 The Data Protection Officer has been appointed to take responsibility for TouchByte's compliance with this policy on a day-to-day basis, with direct responsibility for ensuring that TouchByte complies with the GDPR in respect of data processing that takes place within their area of responsibility.

3.3 The Data Protection Officer is responsible for the management of personal information within TouchByte and for ensuring that compliance with data protection legislation and good practice can be demonstrated. This accountability includes:

3.3.1 development and implementation of the PIMS as required by this policy;

3.3.2 ensuring that employee responsibilities are set out in individual job descriptions with appropriate training, and

3.3.3 security and risk assessments/management in relation to compliance with the policy.

3.4 Being the owner of this document and ensuring that this policy document is reviewed in line with the review requirements stated below. Mark Bailey, the Data Protection Officer, is a TouchByte Director.

3.5 The Data Protection Officer is responsible, each year, for reviewing the details of ICO notification, in the light of any changes to TouchByte's activities (as determined by changes to the Data Inventory Register and the management review) and to any additional requirements identified by means of DPIA (see 4)

3.6 The Data Protection Officer have specific responsibilities in respect of procedures such as the Subject Access Request Procedure and as the first point of call for Employees seeking clarification on any aspect of data protection compliance.

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

4. Data Protection Risk Assessment (DPIA)

4.1 The objective of a DPIA is to ensure that TouchByte is aware of any risks associated with the processing of particular types of personal information.

4.2 TouchByte 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 undertaken by other organisations on behalf of TouchByte. TouchByte shall manage any risks which are identified by the risk assessment in order to reduce the likelihood of a non-conformance with this policy.

4.3 Where a type of processing, in particular using 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, TouchByte shall, prior to the processing, carry out a DPIA to assess the impact of the envisaged processing operations on the protection of personal data.

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

4.5 Where, as a result of a DPIA, it is clear that TouchByte 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 TouchByte may proceed must be escalated for review to Board of Directors.

4.6 Appropriate controls will be selected [from ISO27001 Annex A] and applied to reduce the level of risk associated with processing individual data to an acceptable level, by reference to the requirements of the GDPR.

5. <u>Data protection principles</u>

5.1 All processing of personal data must be done in accordance with the following data protection principles of the Regulation, and TouchByte's policies and procedures are designed to ensure compliance with them.

5.2 Personal data must be processed lawfully, fairly and transparently. The GDPR requires that the controller has 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. The specific information that must be provided to the data subject must as a minimum include:

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

5.2.2 the contact details of the Data Protection Officer, where applicable;

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

5.2.4 the period for which the personal data will be stored;

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

5.2.6 the categories of personal data concerned;

5.2.7 the recipients or categories of recipients of the personal data, where applicable;

5.2.8 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;

5.2.9 any further information necessary to guarantee fair processing.

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

5.4 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 TouchByte's GDPR registration. GDPR DOC 2.1 sets out the relevant procedures.

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

5.5.1 The Data Protection Officer is responsible for ensuring that information which is not strictly necessary for the purpose for which it is obtained, is not collected.

5.5.2 All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must be approved by the Data Protection Officer.

5.5.3 The Data Protection Officer will ensure that, on an annual basis, all data collection methods are reviewed by internal audit to ensure that collected data continues to be adequate, relevant and not excessive.

5.5.4 If data is given or obtained that is excessive or not specifically required by TouchByte's documented procedures, the Data Protection Officer is responsible for ensuring that it is securely deleted or destroyed in line with the Secure Deletion Policy.

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

5.6.1 Data that is kept for a long time must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.
5.6.2 The Data Protection Officer is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.
5.6.3 It is also the responsibility of individuals to ensure that data held by TouchByte is accurate and up-to-date. Completion of an appropriate registration or application form etc will be taken as an indication that the data contained therein is accurate at the date of submission.
5.6.4 Employees/Customers/Others should notify TouchByte of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of TouchByte to ensure that any notification regarding change of circumstances is noted and acted upon.
5.6.5 The Data Protection Officer 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.
5.6.6 On at least an annual basis, the Data Protection Officer will review all the personal data maintained by TouchByte, 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 in line with the Secure Deletion Policy.

5.7 The Data Protection Officer is responsible for making appropriate arrangements that, where third party organisations may have been passed inaccurate or out-of-date personal information, for information them that the information is inaccurate and/or out-of-date and is not to be used to inform decisions about the individuals concerned; and for passing any correction to the personal information to the third party where this is required.
5.8 Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.

5.8.1 Where personal data is retained beyond the processing date, it will be minimized and/or encrypted in line with the Information Security Policy in order to protect the identity of the data subject in the event of a data breach.
5.8.2 Personal data will be retained in line with the Retention of Records Policy and, once its retention date is passed, it must be securely destroyed as per the Secure Deletion Policy.
5.8.3 The Data Protection Officer must specifically approve any data retention that exceeds the retention periods defined in Data Inventory Register, and must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation.

5.9 Personal data must be processed in a manner that ensures its security.
5.10 Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed. TouchByte's compliance with this principle is contained in its Information Security Policy.
5.11 Personal data shall not be transferred to a country or territory outside the European Union 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. The transfer of personal data outside of the EU is prohibited unless one or more of the specified safeguards or exceptions apply.
5.12 Safeguards. An assessment of the adequacy by the data controller taking into account the following factors:

- the nature of the information being transferred;
- the country or territory of the origin, and final destination, of the information;
- how the information will be used and for how long;
- the laws and practices of the country of the transferee, including relevant codes of practice and international obligations; and
- the security measures that are to be taken as regards the data in the overseas location.

5.13 Binding corporate rules

TouchByte may adopt approved Binding Corporate Rules for the transfer of data outside the EU. This requires submission to the relevant Supervisory Authority for approval of the rules that TouchByte is seeking to rely upon.

5.14 Model contract clauses

TouchByte may adopt approved model contract clauses for the transfer of data outside of the EU. If TouchByte adopts the model contract clauses approved by the relevant Supervisory Authority there is an automatic recognition of adequacy.

5.15 Exceptions

In the absence of an adequacy decision, including binding corporate rules, a transfer of personal data to a third country, or an international organisation, shall take place only on one of the following conditions:

- the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims;
- the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;
- the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case.

A list of countries that satisfy the adequacy requirements of the Commission are published in the *Official Journal of the European Union.*

6. Data subjects' rights

6.1 Data subjects have the following rights regarding data processing, and the data that is recorded about them:

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

6.1.2 To prevent processing likely to cause damage or distress.

6.1.3 To prevent processing for purposes of direct marketing.

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

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

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

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

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

6.1.9 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.

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

6.2 Data subjects may make data access requests as described in the Subject Access Request Form; this procedure also describes how TouchByte will ensure that its response to the data access request complies with the requirements of the Regulation.

6.3 Data subjects who wish to complain to TouchByte about how their personal information has been processed may lodge their complaint directly with the Data Protection Officer by means of an email to sales@touchbyte.co.uk or via post at TouchByte Ltd, The FibreHub, Trevenson Lane, Pool, Redruth, Cornwall, TR15 3GF.

6.4 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 the Data Protection Officer.

7. Consent

7.1 TouchByte 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.

7.2 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.

7.3 Explicit consent by Data subjects has been captured via Personal Information Processing Consent form. There must be some active communication between the parties which demonstrate active consent. Consent cannot be inferred from non-response to a communication.

7.4 Consent to process personal and sensitive data is generally obtained routinely by TouchByte using standard consent documents e.g., when a new member of staff signs a contract of employment, or during induction for participants on programmes.

7.5 Where TouchByte provides online services to children, parental or custodial authorisation must be obtained. This requirement applies to children under the age of 16 (unless the Member State has made provision for a lower age limit – which may be no lower than 13).

8. Security of data

8.1 All Employees are responsible for ensuring that any personal data which TouchByte 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 TouchByte to receive that information and has completed a Data Confidentially Agreement.

8.2 All personal data is kept according to the Information Security Policy and Acceptable Use Policy.

9. Rights of access to data

9.1 Data subjects have the right to access any personal data (i.e., data about them) which is held TouchByte 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 TouchByte, and information obtained from third-party organisations about that person.

9.2 Subject Access Requests are dealt with as described in Subject Access Request form.

10. Disclosure of data

10.1 TouchByte 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. 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 consider whether disclosure of the information is relevant to, and necessary for, the conduct of TouchByte's business.

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

- to safeguard national security;
- prevention or detection of crime including the apprehension or prosecution of offenders;
- assessment or collection of tax duty;
- discharge of regulatory functions (includes health, safety and welfare of persons at work);
- to prevent serious harm to a third party;
- to protect the vital interests of the individual, this refers to life and death situations.

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 the Data Protection Officer.

11. Retention and disposal of data

Personal data may not be retained for longer than it is required. Once a member of staff has left TouchByte, it may not be necessary to retain all the information held on them. Some data will be kept for longer periods than others. TouchByte's Retention of Records Policy will apply in all cases.

11.1 Disposal of records - 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 Deletion Procedure.

12. Definitions (drawn from the GDPR)

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.

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.

Data controller – the entity that determines the purposes and means of the processing of personal data.

Data subject – any living individual who is the subject of personal data held by an organisation.

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

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 behavior. 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.

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 to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

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.

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.

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.

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.